

The algorithms are done. The deployments are not.

We asked for the unglamorous part: what blocked you, what you tried that did not work, and what is still open. The output is an IAB report that records problems and positions, not a vendor comparison and not consensus.

WHO IS IN THE ROOM

52

submissions to the call for position papers

20

accepted, and about forty people who build, run, or regulate systems that have to authenticate with post-quantum signatures

Success looks like a short list of things the IETF, the IAB, or someone else should do next, with the evidence behind each.

TODAY ONLY

You may use what you hear today. You may not say who said it, or where they work.

- Chatham House rule. Notes and the report will say "a participant", "an operator", "a CA". Never a name or a company.
- No recording, no photos of slides without asking, no live posting of quotes.
- Day 1 is in person only. Tomorrow at Cisco is different: remote participants join, and the usual attribution applies.

Disagree with the argument, not the person.

- The IETF code of conduct (RFC 7154) and the IETF anti-harassment policy apply here.
- Ask the hard question, then let the answer land.
- Chairs will stop people at time and will call on people who have not spoken. That is the job, not a judgement.
- If something is wrong, tell Nick or Yaroslav, in the room or on Slack.

FORMAT

Ten minutes to present.

Each session: the chair frames the theme in a minute, then each talk gets ten minutes with a hard stop.

Slides are on one laptop. If yours is not there yet, send it to pq-workshop-pc@iab.org now.

The discussion is the product.

Sixty to ninety minutes of moderated discussion on the whole theme, steered toward blockers, failed attempts, and open questions.

Five minutes before the end, the chair asks for two or three takeaways. Those go straight into the report. Anything off-theme goes to the parking lot for the wrap-up.

DAY 1 AGENDA, TIMES IN CEST

TIME	SESSION	TALKS	CHAIR
09:00	Welcome and introductions	Everyone, one line each	Nick
09:30	National ID and Digital Identity	UK GDS, D-Trust	Vladimir
10:50	Break		
11:20	Performance and Embedded Systems	PQShield, Zscaler, Aleutian AI	Mike O
13:20	Lunch, delivered to the room		
14:20	Code Signing, Keys and Hardware	GitHub/npm, Siemens, Facti, Crypto4A	Murugiah
16:30	Wrap-up	Takeaways, parking lot, tomorrow	Nick
17:00	End of Day 1		

TODAY AT CTU

- Coffee, tea, water and biscuits are in the room all day.
- Lunch arrives at 13:00: boxed baguettes and salads, with vegetarian and vegan options.
- Entrance is through the Faculty of Civil Engineering. Jaroslav will point out toilets and exits.
- Slack: pqauthiabworkshop.slack.com, channel `all-pq-auth-iab-workshop`, for questions during the day.
- Notes: Nick is scribing in a shared doc. Chairs have the link. Corrections welcome any time.
- Tomorrow: Cisco, Pujmanove 1753/10a, Pankrac metro, line C. Lobby opens 08:30, bring ID. Lunch is on your own.

INTRODUCTIONS, THIRTY SECONDS EACH

- 1 Who you are and what you run or build.
- 2 The one thing about post-quantum authentication you most want an answer to this weekend.

Forty people times thirty seconds is twenty minutes. Hold the detail for the sessions; Nick keeps time.

16:30 WRAP-UP

- 1 What blocks you from deploying post-quantum authentication today?
- 2 What did you hear today that changed your plan?
- 3 What should the IETF or the IAB do next, and what should they leave alone?

Then the parking lot, then tomorrow's logistics. Thank you to CESNET and CTU for the room.