

Accelerating the Deployment of Post-Quantum Authentication

IAB Workshop, Day 1

Sunday 11 October 2026, Czech Technical University, Prague

Date

Note Well

- ❖ This is a reminder of IETF policies in effect on topics such as patents and code of conduct. It only points you in the right direction; exceptions may apply. The patent policy and the definitions of an IETF contribution and participation are in BCP 79.
- ❖ By participating you agree to follow IETF processes and policies.
- ❖ If you know that any contribution is covered by patents or patent applications owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- ❖ Written, audio, video and photographic records of meetings may be made public. Personal information is handled under the IETF Privacy Statement.
- ❖ Work respectfully with other participants; contact the ombudsteam with questions or concerns.
- ❖ Definitive information: BCP 9 (standards process), BCP 25 (working group processes, anti-harassment), BCP 54 (code of conduct), BCP 78 (copyright), BCP 79 (patents).

The algorithms are done. The deployments are not.

- ❖ 52 submissions to the call for papers, 20 accepted, about forty people in this room
- ❖ Every one of you runs, builds, or regulates something that has to authenticate with post-quantum signatures
- ❖ We asked for the unglamorous part: what blocked you, what you tried that did not work, what is still open
- ❖ The output is an IAB workshop report: problems and positions, not a vendor comparison and not consensus
- ❖ Success is a short list of things the IETF, the IAB, or someone else should do next, with the evidence behind each

Today only: the Chatham House rule

- ❖ You may use what you hear today. You may not say who said it, or where they work.
- ❖ 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 the presenter, no live posting of quotes
- ❖ Day 1 is in person only; there is no remote link
- ❖ Tomorrow at Cisco is different: remote participants join on Webex, and the usual attribution applies

Robust, and respectful

- ❖ The IETF code of conduct (RFC 7154) and the IETF anti-harassment policy apply here
- ❖ Disagree with the argument, not the person. 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
- ❖ And have some fun. It is a Sunday a long way from home.

Format: ten minutes to present, then the real work

- ❖ Each session: the chair frames the theme in a minute, then each talk gets ten minutes with a hard stop
- ❖ Then 60 to 90 minutes of moderated discussion on the whole theme
- ❖ Chairs steer 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.
- ❖ Slides are on one laptop. If yours is not there yet, send it to pq-workshop-pc@iab.org now.
- ❖ Anything off-theme goes in the parking lot for the wrap-up

Day 1 agenda (times in CEST)

- ❖ 09:00 Welcome and introductions (Nick)
- ❖ 09:30 National ID and Digital Identity: UK GDS, D-Trust (chair: Vladimir)
- ❖ 10:50 Break
- ❖ 11:20 Performance and Embedded Systems: PQShield, Zscaler, Aleutian AI (chair: Suresh)
- ❖ 13:20 Lunch, delivered to the room
- ❖ 14:20 Code Signing, Keys and Hardware: GitHub / npm, Siemens, Facti, Crypto4A (chair: Murugiah)
- ❖ 16:30 Wrap-up: takeaways, parking lot, tomorrow (Nick)
- ❖ 17:00 End of Day 1

Links

- ❖ Agenda: [intarchboard.github.io / iab-pq-ws.github.io](https://intarchboard.github.io/iab-pq-ws.github.io)
- ❖ Papers and slides: [datatracker.ietf.org / group / pqws / materials](https://datatracker.ietf.org/group/pqws/materials)
- ❖ Slack: pqauthiabworkshop.slack.com, channel #all-pq-auth-iab-workshop
- ❖ Slides to: pq-workshop-pc@iab.org
- ❖ Chairs: notes doc link is in the PC email

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
- ❖ Wifi: details from Jaroslav
- ❖ 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
- ❖ Notes: Nick is scribing in a shared doc; chairs have the link; corrections welcome any time
- ❖ Tomorrow: Cisco, Pujmanové 1753 / 10a, Pankrác metro (line C). Lobby opens 08:30, bring ID. Lunch on your own.

Introductions: thirty seconds each

- ❖ Who you are and what you run or build
- ❖ The one thing about post-quantum authentication you most want an answer to this weekend
- ❖ Forty people times thirty seconds is twenty minutes, so hold the detail for the sessions. Nick keeps time.

16:30 wrap-up: three questions for the room

- ❖ What blocks you from deploying post-quantum authentication today?
- ❖ What did you hear today that changed your plan?
- ❖ 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.