

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.



Post-Quantum Transition Exercises



CHES matchmaking event
4.2.2025, Brno

Petr Muzikant petr.muzikant@cyber.ee

Jan Willemsen jan.willemsen@cyber.ee

Information Security Research Institute @ Cybernetica AS, Estonia

Our Goals

- Implement PQC in existing applications
- Collect engineering obstacles and solutions
- Follow global standardization efforts (NIST, IETF, ETSI, ...)
- Contribute to the open-source
- Engage in international collaboration outside of Czechia+Estonia
- Disseminate

PQ Projects

- **Web-eID (client authentication)**
 - server, middleware, client
- **CDOC2 (content encryption)**
 - scenarios with and without key exchange server
- **IVXV (e-voting)**
 - almost every aspect of cryptography in one form or another
- **eID (certificates, OCSP, TSA)**
 - backbone of everything else
- **supporting projects**
 - library wrappers, lattice-helper, custom protocols

Next Steps

- PQ e-voting
- Crypto-agile fork of go/crypto (including PQ implementation)
- Toolbox for creating PQ ASiC-E containers
- Explore/develop PQ-TLS solutions


Obtained Experience

- Available technology, libraries, applications
- PKI components: CA, OCSP, TSA, etc..
- HSMs, hardware acceleration, **smart cards**, auth. tokens
- PQC Migration as an IT modernization (**crypto-agility**)
- **Cryptography inventory discovery**
- Engineering obstacles
- **Hybrid modes**
- Hash-then-sign dilemma
- **Others' use cases**


Thank you for your attention!

Petr Muzikant petr.muzikant@cyber.ee

Jan Willemson jan.willemson@cyber.ee


 <https://cyber.ee/>

 info@cyber.ee

 [cybernetica](https://twitter.com/cybernetica)

 [CyberneticaAS](https://www.facebook.com/CyberneticaAS)

 [cybernetica_ee](https://www.instagram.com/cybernetica_ee)

 [Cybernetica](https://www.linkedin.com/company/Cybernetica)