

Summary and closing



PKI
Consortium

Status

- Quantum computers will be able to break current public key encryption
- Accurate crypto inventory & mitigation strategies are required
- Long term data needs to be protected now
- Failure to migrate leaves applications and data at risk of compromise
- This crypto migration will be the hardest we've ever done

What can/should you do now?

Now is the time to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms

- Determine the value of your data, its shelf life, and how long it will take to migrate to post-quantum cryptography.
- Start testing with algorithms identified for standardization
- Plan your migration to post-quantum cryptography
- Do not adopt PQC in production systems until recommended
- Get help and expertise

Crypto Agility

- Know your regulatory compliance requirements
- Know what crypto you use and where
- Do not hardcode algorithms, make it configurable
- Consider that increased size of signatures and keys for data storage, fields with limited sizes, bandwidth, etc.
- Consider that a change in algorithms might slow down your application or systems
- Keep updating your crypto libraries, start phasing out software that is no longer supported
- Implement a Certificate Lifecycle Management (CLM) system
- Use a Key Management System (KMS)

Shall we do this again?



PKI
Consortium

PQC Conference

- Follow-up conference in Europe
- After the summer of 2023
 - Exact date to be confirmed
- This event will be longer, it might even span multiple days, with several tracks, technical and non-technical speakers
- Tracks might cover:
 - Government
 - Hardware
 - Hardware Security Modules (HSMs)
 - Constraint devices (IoT)

Call for presentations

pkic.org/call



pkic.org/call

Sponsor the PKI Consortium

pkic.org/sponsors



pkic.org/sponsors

Thank you and we hope to
see you next time!

<https://pkic.org/join> | feedback@pkic.org



PKI
Consortium