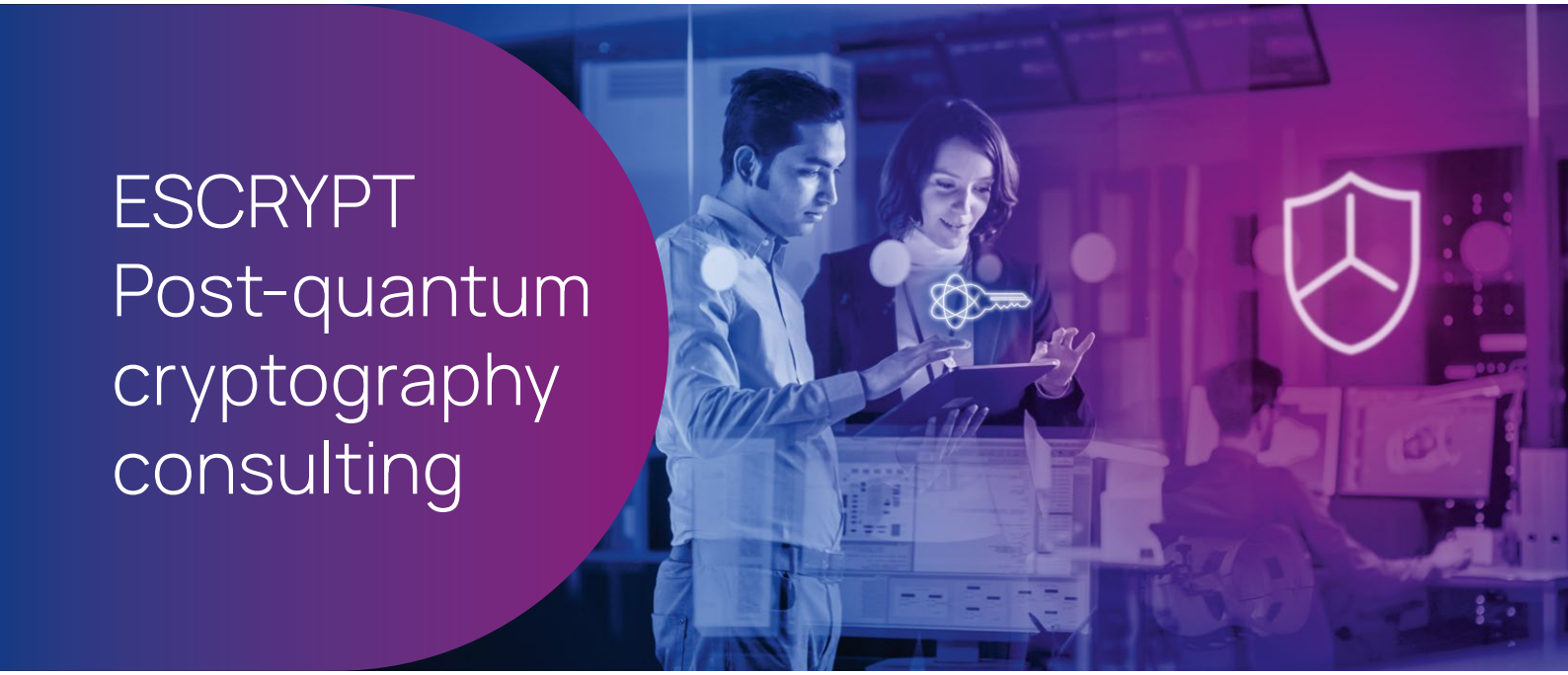
ESCRYPT Post-quantum cryptography consulting



Are you post-quantum ready?

Asymmetric cryptography is now in widespread use, but algorithms that are secure today will be broken by the quantum computers of tomorrow. Although a breakthrough in quantum computing might be some years away, companies need to prepare for the smooth transition to quantum-secure systems in good time. Finding suitable post-quantum algorithms and migrating to quantum-secure systems can pose many challenges.

In addition to our proven expert knowledge in developing secure automotive architectures, ETAS has gained extensive experience in post-quantum cryptography (PQC) as a partner in FLOQI (full lifecycle post-quantum PKI) – a funded project that focuses on developing a post-quantum PKI for automotive use cases, among others.

The challenge

There have been huge advances in quantum computing in recent years and the first computer capable of breaking today's asymmetric cryptography may be here less than ten to fifteen years. Companies using asymmetric cryptography to secure products with long lifecycles need to start looking for secure alternatives now.

Impacts for automotive security

Most of todays and upcoming automotive security measures (e. g. ECU integrity protection, secure onboard communication, V2X, access control etc.) rely on classical cryptography that will be vulnerable to quantum computing.

OEMs in particular need to think about post-quantum cryptography solutions now if they want to avoid disruptions and comply with future standards and legislation applicable to automotive security (e. g., BSI, UN-R 155).

Our recommendations

- Be prepared for the post-quantum world early, before scalable quantum computers exist
- Develop crypto agility and migration solutions (e. g. hybrid PQC solutions), identify suitable algorithms for every use case
- Use existing PQC expertise & implementations, available with trainings, consultations, testing and products like ESCRYPT CycurLIB

ESCRYPT post-quantum cryptography consulting – service overview

Guidance for management

- We offer customer workshops that aim to raise awareness of the problems arising from the development of quantum computers.
- We give specific recommendations on points of action and prioritization, and help you establish a timeline.
- We perform an analysis of the state-of-the-art regarding standardization activities for post-quantum algorithms.

Specific technical quantum-safe solutions

- Our post-quantum cryptography experts analyze specific systems (e. g. function or function clusters) that use asymmetric cryptography in order to identify the changes necessary for migration to post-quantum solutions, taking specific requirements into consideration.
- We design migration and transition solutions, e. g. for the PKI or key management.

Integrating post-quantum solutions into E/E architectures

Our post-quantum cryptography experts analyze post-quantum algorithms with respect to

- Key and signature sizes
- Performance of signing and verifying algorithms
- Memory consumption
- Confidence in security of algorithms
- Use case requirements

We compare resources of deployed ECUs with available benchmarks in order to identify suitable algorithms for different targets/use cases and we offer an analysis of adjacent IT systems (e. g. PKI, backend) with respect to the changes required for post-quantum security.

Your benefits with ESCRYPT PQC consulting

- **Proven expert knowledge:** benefit from years of experience in PQC and automotive security.
- **Latest research insights:** as part of FLOQI, ETAS works together with the project partners on defining a quantum-secure PKI, taking into consideration the needs and specific requirements of the automotive industry.
- **State-of-the-art:** use existing PQC implementations for testing & benchmarking quantum-safe security for embedded & backend systems such as ESCRYPT CycurLIB.
- **Field-proven solutions:** we provide tested and proven solutions to make your systems quantum-secure.

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/pqc-sonsulting

ETAS/COM2_AS/12/2022