



# CELTIC-NEXT



## Proposers Brokerage Day

11<sup>th</sup> September 2025, Aveiro

**SPARC**

Secure **P**ost-quantum **A**rchitecture for **R**esilient **C**harging

**SPARC**



**Dr. Faruk SARI**

Cyber Quanta

[faruk.sari@cyber-quanta.com](mailto:faruk.sari@cyber-quanta.com)



## Main Benefit:

*A practical Post-Quantum Cryptography (PQC) upgrade path for EV charging stations — securing the smart grid against quantum threats.*



## Added Value:

- *Real-world performance benchmarks for next-gen quantum-safe encryption.*
- *Future-proof EV charging protocols with embedded PQC.*
- *Trusted key protection using secure hardware (HSM/TEE).*



## Why Join:

*Help shape Europe's PQC-ready EV infrastructure — standards-based, future-proof, and open-source-driven.*

# Organisation Profile



- Deep-tech **SME** focused on **Post-Quantum Cryptography**, secure IoT, and critical infrastructure protection
- Based in **Teknopark İstanbul**, operating across EU and international markets
- Led by founders with **55+ years of combined experience** in cybersecurity and cryptography
- Builds **quantum-safe, regulation-aligned** solutions (CRA, GDPR) and contributes to global PQC transition efforts

# Proposal Introduction

*Quantum Risk Is Real — and Closer Than You Think*



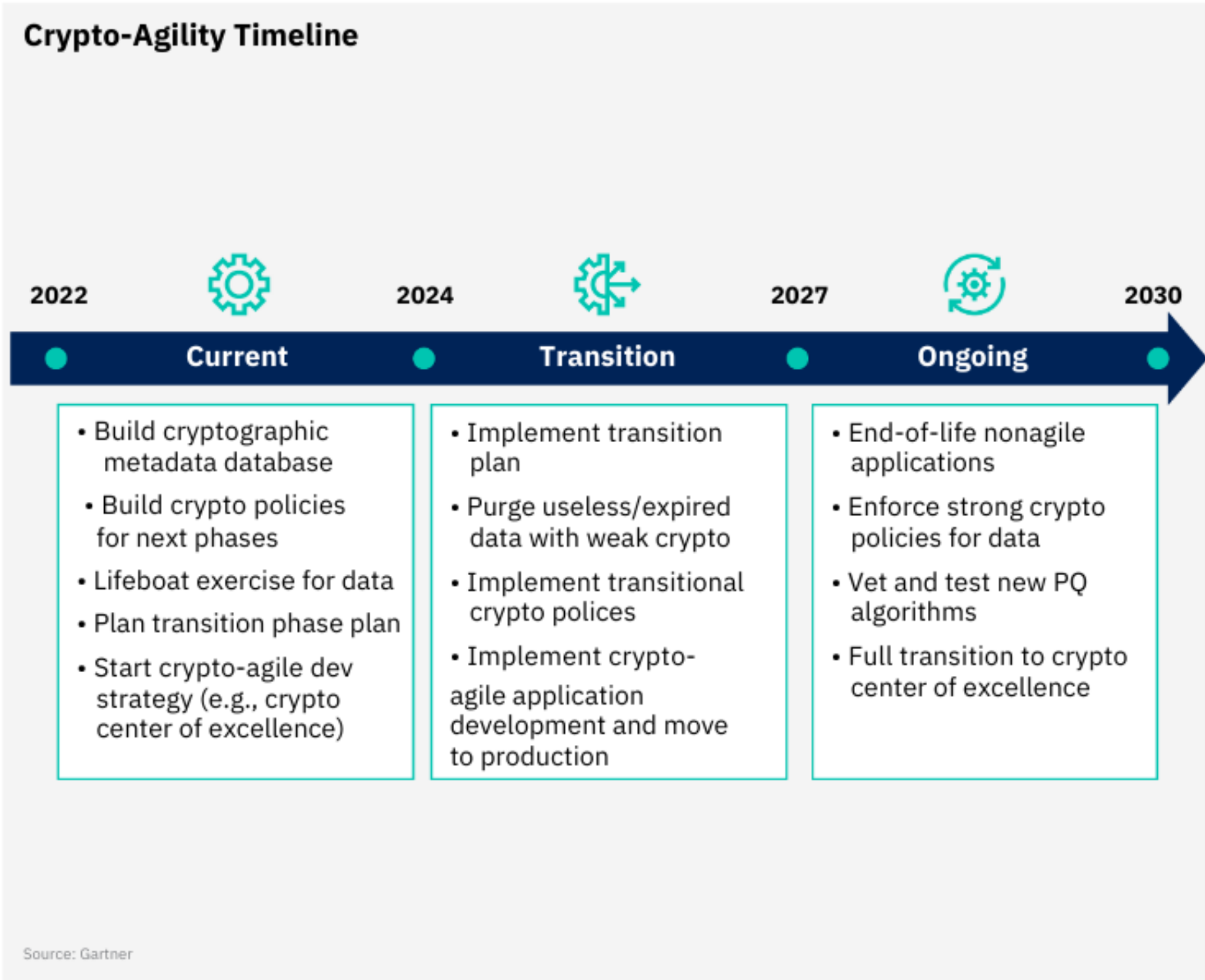
New frontiers of computing 

4

Post-Quantum Cryptography

Post-quantum cryptography (PQC) refers to cryptographic methods designed to be secure against the potential threats posed by quantum computers.

For more on how it works and how to get started, read: "What Is Post-Quantum Cryptography?"



# Proposal Introduction

## Vision & Motivation

- Future-proof EV charging infrastructure against quantum threats.
- Comply with EU CRA, NIS2, GDPR.

## Core Idea

- Integrate PQC (ML-KEM, HAWK, etc.) into ISO 15118 & OCPP.
- Benchmark on EVSE hardware + secure keys via HSM/TEE.

## Impact

- Efficient, scalable path to quantum-safe smart grids.



# Proposal Introduction

## Expected Outcomes

- PQC-enabled protocol extensions for ISO 15118 & OCPP
- Benchmarked lightweight PQC algorithms (ML-KEM, HAWK, MQOM...) on EVSE smart meters
- Embedded secure key management using HSM/TEE

## Expected Impact

- Accelerates PQC transition in critical smart grid infrastructure
- Contributes to European PQC standards and open-source ecosystem
- Enhances compliance with EU-CRA, NIS2, and future PQC mandates

## Schedule (36 Months)

- Months 1–6: PQC scheme selection, embedded HW setup
- Months 7–18: Implementation & benchmarking
- Months 19–30: Protocol extension, key mgmt prototyping
- Months 31–36: Testing, documentation, standardization input

# Partners



## Consortium Members

- Cyber Quanta (Türkiye): *System integration, PQC migration, secure key management*
- University of Tartu (Estonia): *PQC algorithm evaluation, cryptographic benchmarking*

## Looking For Partners With Expertise In:

- Electric vehicle charging systems, OCPP/mobility platforms, and secure protocol stack development
- Embedded system design teams capable of secure boot, filesystem encryption, and integration of hardware-based secure elements on Linux platforms
- Companies with experience in secure IoT device manufacturing and field deployment of cryptographic hardware

# Contact Info

**For more information and for interest to participate please contact:**

**Dr. Faruk SARI**, Cyber Quanta



[faruk.sari@cyber-quanta.com](mailto:faruk.sari@cyber-quanta.com)



+90 216 212 55 40



Teknopark Istanbul, NO: 1 /4C-213- Pendik/ ISTANBUL



[www.cyber-quanta.com](http://www.cyber-quanta.com)



**Presentation is available via:**



# Join the Consortium Building Sessions

**17. September**  
**from 09:00-09:45 CET**

Connection details:  
Via

[www.celticnext.eu/new-ideas](http://www.celticnext.eu/new-ideas)

