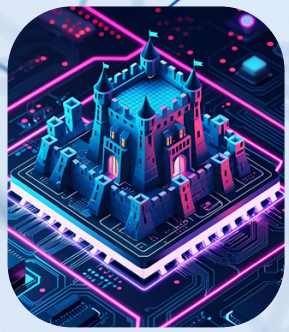
Context & Challenges



The foundation of modern cybersecurity lies in the secure boot process, ensuring only trusted and authenticated software runs on a device. By validating code integrity through cryptographic signatures, secure boot upholds the Confidentiality, Integrity, and Availability triad, acting as the first line of defence against tampering, malware, and unauthorised changes.

Currently, secure boot relies on traditional cryptographic algorithms like RSA. However, the advent of quantum computing poses a threat to these systems, as quantum algorithms like Shor's could compromise them, necessitating a transition to Post-Quantum Cryptography. The European Union and relevant agencies, such as ANSSI and BSI, advocate for a Post-Quantum/Traditional (PQ/T) hybrid cryptographic model, combining quantum-resistant algorithms with traditional cryptography for added resilience. Implementing quantum-safe secure boot remains challenging due to the performance, scalability, and compliance trade-offs of PQ/T solutions.

Subscribe to our newsletter

FORTRESS Partners

FORTRESS Kick-Off meeting in Germany, 7-8 Oct. 2025

FORTRESS is a HORIZON-CL3-2024-CS-01 project that has received funding from the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under the European Commission under the grant agreement number 101225722.

https://pq-fortress.eu/

@FORTRESS project

@FORTRESSFO91233

@FORTRESS_Project

zenodo.org/communities/fortress_project/

FORTRESS

FULLY OPTIMISED ROOT OF TRUST FOR ROBUST EMBEDDED SECURITY SYSTEMS

https://pq-fortress.eu/

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

About FORTRESS

FORTRESS aims to address challenges of modern cybersecurity by developing a scalable and efficient hybrid secure boot architecture.

It will design a flexible Root of Trust that integrates both traditional and post-quantum algorithms, while exploring trade-offs between security, performance, and cost.

Objective 1 – KPI Exploration

Develop a benchmarking framework for PQ/T hybrid secure-boot systems to evaluate trade-offs in security, cost, & performance.

Objective 2 – PQ/T Hybrid Root of Trust

Design a flexible, CHERI-enabled PQ/T Hybrid Root of Trust integrating hardware and software components.

Objective 6 – Dissemination, Standardisation, & Exploitation

Maximise impact by promoting FORTRESS innovations across industry, academia, and standardisation bodies.

6 Objectives

to address challenges of modern cybersecurity.

The project balances security, performance, & cost, for a smooth migration to quantum-resilient architectures across Europe.

Objective 3 – Secure Boot Demonstrator

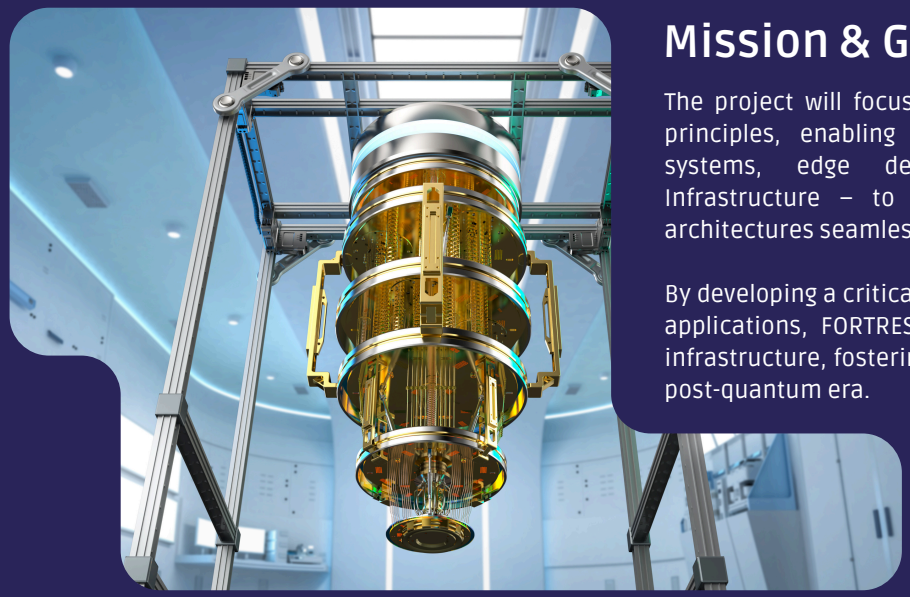
Showcase real-world secure boot implementations for IoT/Edge and CNI environments.

Objective 5 – Trusted Communications Platform

Provide security testing and validation tools to support large-scale PQC adoption.

Objective 4 – Security Tool Deployment

Provide security testing and validation tools to support large-scale PQC adoption.



Mission & Goals

The project will focus on hardware-software co-design principles, enabling diverse platforms – embedded systems, edge devices, and Critical National Infrastructure – to transition to quantum-resistant architectures seamlessly.

By developing a critical building block for a wide range of applications, FORTRESS will safeguard Europe's digital infrastructure, fostering resilience and leadership in the post-quantum era.

Additionally, the project will engage industry stakeholders to align with regulatory and standardisation efforts, ensuring practical deployment and maximum impact.

Ambition & Impact

FORTRESS advances the state of the art by combining post-quantum cryptography with hardware-enforced security to deliver trusted systems that remain secure in the quantum era.

The project contributes to EU leadership in PQC standardisation, ensures the resilience of critical infrastructures, and enables a secure digital transition for industries and public services across Europe.

Consortium

EURESCOM – Innovation through Collaboration

cyberhive

eShard

Codasip

PQ SHIELD

Universität der Bundeswehr München