



www.xtrust-6g.eu

## About

# XTRUST-6G

As 6G networks take shape, ensuring their security, resilience, and trustworthiness is more critical than ever.

The XTRUST-6G project is at the forefront of securing next-generation wireless communications by integrating cutting-edge technologies such as zero-trust security, quantum-safe cryptography, and AI-driven cyber defense.

Coordinated by CERTH, this initiative brings together 19 leading organizations from 12 countries, working collectively to enhance the safety and reliability of future networks.

Pioneering Next-Generation  
6G Cybersecurity Frameworks

www.xtrust-6g.eu

## WHO

# WE ARE

19 Partners  
12 Countries  
36-Month Project

COORDINATED BY:

CERTH - Centre  
for Research & Technology  
Hellas (Greece)

## PARTNERS



### CONTACT:

info@xtrust-6g.eu

### STAY CONNECTED & FOLLOW US ON:

@XTRUST6G

@XTRUST-6G-HORIZON

@XTRUST-6GHORIZON



X TRUST-6G



Extended Zero-Trust  
and Intelligent Security  
for Resilient & Quantum-Safe  
6G Networks

www.xtrust-6g.eu



This work is a part of the XTRUST-6G project. XTRUST-6G is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Smart Networks and Services Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

### Project funded by

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra  
Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

## Key Objectives

XTRUST-6G focuses on pioneering security solutions tailored for the unique demands of 6G environments.

The project aims to:

Develop **Zero-Trust Security** architecture to **increase resilience**

Provide **risk-based situational awareness** with **proactive security tools**

Implement **AI-based zero-touch E2E protection**

Enhance visibility, control, monitoring and security orchestration

Ensure trustworthy operations using **blockchain** for **identity verification, lifecycle management & compliance**

Secure the **5G+/6G supply chain** by establishing an **OSS security framework & AI-driven risk-based detection and remediation**



The next-generation **Cybersecurity tools**



## Key Innovations

The XTRUST-6G introduces six key innovations to revolutionize the security of 5G+/6G networks:

- 01 **Zero-trust security**, enabling **real-time risk-based access control** to strengthen **6G resilience**, reduce **cyber breaches**, and enhance **public trust**.
- 02 **Collaborative extended detection and response (C-XDR)** improving **situational awareness**, reducing **attack response time** and safeguarding European supply chains.
- 03 **Blockchain-powered identity verification** ensuring **tamper-proof digital identities and secure O-RAN asset lifecycle management** and reinforcing EU digital sovereignty.
- 04 **Quantum-safe cryptography (QKD, PQC)** safeguarding 6G networks against physical layer attacks.
- 05 **Cyber deception techniques**, such as AI-driven honeypots, **enhancing intrusion detection and preventing costly data breaches**.
- 06 **Federated learning and graph-based threat modelling** enabling **privacy-preserving AI security and collaborative threat intelligence sharing**, while AI-powered automation optimizes **energy efficiency**, aligning with **EU Green Deal's objectives**.

## Pilots

To validate these innovations, XTRUST-6G will conduct five pilot deployments across multiple sectors, demonstrating real-world security applications:

- 01 **6G-enabled EV charging infrastructure resilience** – Integrates 5G/6G into EV charging with zero-trust and zero-touch security, ensuring reliable network slices, congestion prevention and enhanced communication via O-RAN mechanisms
- 02 **Safeguarding 6G-connected autonomous vehicles** – Enables AI-driven cyber-attack assessment in Autonomous Vehicles and secures smart mobility by protecting 5G+/6G infrastructure with encrypted communication, policy-based authorization and collaborative security
- 03 **Quantum key distribution for end-to-end 6G security** – Ensures 6G security through QKD-based encryption for authenticated E2E communication and secure backhaul links
- 04 **Securing UAV-assisted 6G communications** – Enhances UAV security in 5G+/6G with encrypted communication, audit mechanisms and physical-layer protection strengthening resilience against attacks
- 05 **Securing O-RAN & Virtualized 6G infrastructure** – Protects O-RAN systems with intrusion detection, zero-touch security orchestration and software supply chain security for cloud and edge applications

These pilots will provide crucial insights into how 6G security solutions perform in different environments.