XTRUST-6G

Press Release

XTRUST-6G: Advancing Secure and Resilient 6G Networks

Europe, June 2025 – As 6G technology continues to evolve, the *XTRUST-6G* project has been launched to tackle one of the most critical challenges: ensuring the security and resilience of next-generation wireless communication networks. Coordinated by the *Centre for Research & Technology* Hellas *(CERTH)*, this collaborative initiative unites 19 partners from 12 countries across Europe and beyond. Together, they aim to develop secure, scalable, and efficient solutions for 6G networks, with a strong focus on quantum-safe security frameworks.

As the demand for ultra-secure, low-latency, and energy-efficient networks grows, *XTRUST-6G* seeks to lay a solid foundation for 6G by introducing a zero-trust security architecture. The project's primary goal is to enhance network protection against evolving cyber threats through AI-driven risk management, real-time cyber threat intelligence, and automated security measures. Additionally, the project incorporates quantum-safe technologies such as Quantum Key Distribution (QKD) to safeguard data transmission from the potential risks posed by future quantum computing advancements.

Key Objectives and Innovations

The *XTRUST-6G* project is focused on the following objectives:

- **Development of zero-trust security architectures** to mitigate cyber threats in dynamic 6G environments.
- **Introduction of quantum-safe encryption methods**, including Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), to counteract the risks posed by quantum computing.
- **Integration of AI and machine learning-driven solutions** for efficient intrusion detection, reducing attack surfaces, and preventing unauthorized access.
- **Enhancement of privacy-preserving AI/ML frameworks** to ensure fairness, sustainability, and minimal environmental impact.

Real-World Testing and Pilots

The project will validate its security solutions through five large-scale pilots in diverse sectors, including autonomous vehicles, electric vehicle (EV) charging infrastructure, and Unmanned Aerial Vehicles (UAVs)-assisted 6G communications. These pilots will offer practical insights into the effectiveness of the proposed security measures and ensure the resilience of 6G networks against emerging cyber threats.

The key pilots include:

- **6G-enabled EV Charging Infrastructure**: Securing electric vehicle charging stations across Europe.

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. It has also 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

- **Securing 6G-connected Autonomous Vehicles**: Strengthening the resilience of autonomous transport systems in smart cities.
- **Quantum Key Distribution for 6G Security**: Exploring quantum encryption methods for secure communications.
- **UAV-assisted Communications**: Enhancing the security of drone communications in critical operations like surveillance and environmental monitoring.
- **O-RAN and Virtualized 6G Infrastructure Security**: Securing cloud-based 6G networks and distributed environments.

These pilots will be deployed across several European locations, including Greece, Estonia, and Luxembourg, allowing the project to test its security measures in real-world settings.

Project Collaboration

XTRUST-6G brings together a multidisciplinary consortium of partners spanning industry, academia, and applied research. The project unites leading technology providers, telecom operators, universities, and research institutions across Europe, all contributing their expertise to address the complex security and privacy challenges of 6G networks. This collaborative effort ensures a comprehensive approach to developing, testing, and deploying advanced cybersecurity solutions for next-generation communication systems.

For more information about the *XTRUST-6G* project and its partners, please visit: www.xtrust-6g.eu

Find and join us online | LinkedIn: xtrust-6g-horizon | **X:** XTRUST6G

Contact Details:

- XTRUST-6G Project Coordinator (CERTH –Center for Research & Technology Hellas): Dr. Stefanos Vrochidis, Dimitris Kavallieros – xtrust6g_coo@iti.gr
- XTRUST-6G Communications & Dissemination Manager (INCITES Consulting SA): Dr. Theodoros Rokkas - trokkas@incites.eu, Sophia Adam – s.adam@incites.eu

Project Facts

- **Project Number**: 101192749
- **Project Name**: Extended Zero-Trust and Intelligent Security for Resilient and Quantum-Safe 6G Networks and Services
- **Project Acronym**: XTRUST-6G
- **Call**: HORIZON-JU-SNS-2024
- **Project Duration**: 36 months (Start Date: 1 January 2025)
- **Project Coordinator**: CERTH –Center for Research & Technology Hellas (Greece)

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. It has also 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**

- **Partners**: 19 partners from 12 countries
- **Grant Amount:** 7.998.595,00 Euros
- **Funding Authorities:** XTRUST-6G is co-funded by the European Union. It has also received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Partners

1. CERTH – Centre for Research and Technology Hellas (Greece)
2. UPORT – University of Portsmouth (United Kingdom)
3. EDLUX – European Dynamics Luxembourg SA (Luxembourg)
4. UOP – University of Peloponnese (Greece)
5. K3Y – K3Y (Bulgaria)
6. ADDITESS – Additess Advanced Integrated Technology Solutions & Services Ltd (Cyprus)
7. INCITES – Incites Consulting SA (Luxembourg)
8. HDPA – Hellenic Data Protection Authority (Greece)
9. SMTEC – Summit TEC Group Ltd (Cyprus)
10. UTH – University of Thessaly (Greece)
11. SNT – University of Luxembourg (Luxembourg)
12. ERI – Ericsson Telecomunicazioni SPA (Italy)
13. TALTEC – Tallinn University of Technology (Estonia)
14. PPC – Public Power Corporation S.A. (Greece)
15. IQU – Iquadrat Informatica SL (Spain)
16. TID – Telefónica Innovación Digital SL (Spain)
17. CYEN – Cyentific AS (Norway)
18. TS – Telekom Slovenije DD (Slovenia)
19. SPHYNX – Sphynx Technology Solutions AG (Switzerland)

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. It has also 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**