Project outputs will be validated in three use cases:

Online banking

Activity tracking

Device management

FutureTPM Main Goals

Secure QR Cryptographic Algorithms for TPM

Implementation of Hardware, Software, Virtual TPM

Provision of Run-time Risk Assessment and Vulnerability Analysis

Contact Information:

Project Coordinator:
MMag. Martina TRUSKALLER
TECHNIKON Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Email: coordination@futuretpm.eu

Scientific/Technical Lead:
Prof. Liqun CHEN
University of Surrey
388 Stag Hill
Guildford GU2 7XH
United Kingdom
Email: liqun.chen@surrey.ac.uk

Scientific/Technical Lead:
Dr. Thanassis GIANNETSOS
Technical University of Denmark
Anker Engelunds Vej 1 Bygning 101A
2800 Kgs. Lyngby
Denmark
Email: atgi@dtu.dk

Project:
Total cost: 4,868,890 €
EC contribution: 4,868,890 €
Project start: 1st January, 2018
Duration: 36 months

www.designetica.at

Foto: Shutterstock/alice-photo | Icons: Freepik/www.flaticon.com

FutureTPM: Future Proofing the Connected World
A Quantum-Resistant Trusted Platform Module

www.futuretpm.eu

Main

The **FutureTPM project** is aimed at designing and developing a Quantum-Resistant Trusted Platform Module (TPM). FutureTPM will provide a new generation of TPM-based solutions, including hardware, software and virtualization environments, incorporating robust and physically secured Quantum-Resistant cryptographic primitives. This will allow long-term security, privacy and operational assurance for future ICT systems and services. FutureTPM solutions will also improve the security of Hardware Security Modules, the Trusted Execution Environments, Smart Cards, and the Internet of Things.

Goals

Implementation for hardware, software, and virtual TPM

Secure quantum-resistant cryptographic algorithms for the TPM

Real-world applications to tested industrial use-cases

Design validation using formal security analysis

Standardization within TCG, ISO/IEC and ETSI