FutureTPM

Contact

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

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

Project Partners:

1 **TECHNIKON Forschungs- und Planungsgesellschaft mbH, Austria [Villach]**

2 **University of Surrey, United Kingdom [Guildford]**

3 **UBITECH Limited, Cyprus [Limassol]**

4 **Royal Holloway and Bedford New College, United Kingdom [Egham]**

5 **IBM Research GmbH, Switzerland [Rüschlikon]**

6 **The University of Birmingham, United Kingdom [Birmingham]**

7 **Infineon Technologies AG, Germany [Neubiberg]**

8 **Infineon Technologies Austria AG, Austria [Graz]**

9 **Université du Luxembourg, Luxembourg [Luxembourg]**

10 **Suite5 Data Intelligence Solutions Limited, Cyprus [Nicosia]**

11 **NESC-ID – Instituto de Engenhariade Sistemas e Computadores, Investigacao e Desenvolvimento em Lisboa, Portugal [Lisboa]**

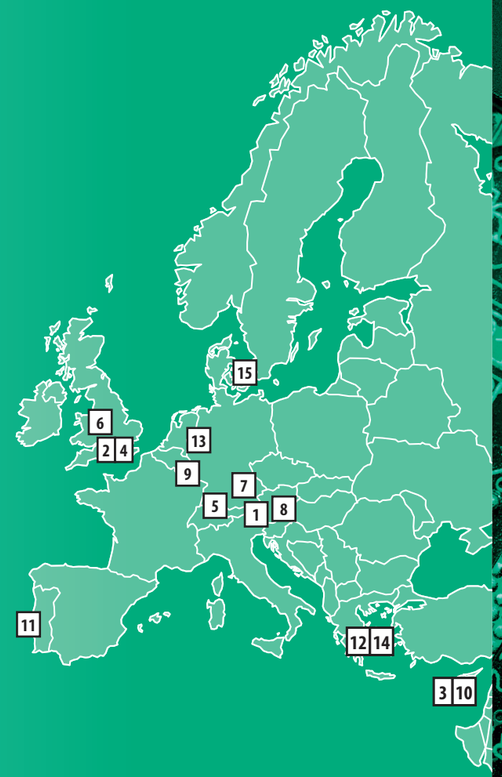
12 **University of Piraeus Research Center, Greece [Piraeus]**

13 **Huawei Technologies Düsseldorf GmbH, Germany [Düsseldorf]**

14 **INDEV Software SA, Greece [Athens]**

15 **Technical University of Denmark, Denmark [Lyngby]**

For more information, please visit https://www.futuretpm.eu



Consortium

The FutureTPM consortium consists of 15 highly qualified industrial and academic partners from a wide variety of backgrounds and from 9 different countries (Austria, Cyprus, Germany, Greece, Lux-embourg, Portugal, Switzerland, United Kingdom and Denmark):

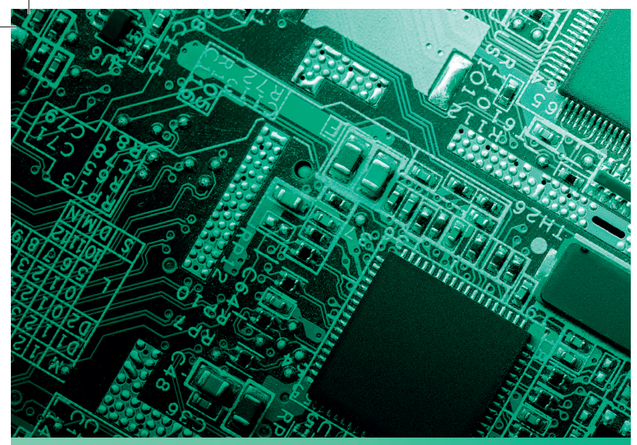
FutureTPM

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

Project number: **779391**
Project website: **www.futuretpm.eu**
Project start: **1st January, 2018**
Duration: **36 months**
Total cost: **EUR 4,868,890**
EC contribution: **EUR 4,868,890**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391.

FutureTPM



The Mission of FutureTPM

The **FutureTPM** project is aimed at designing and developing a Quantum-Resistant (QR) Trusted Platform Module (TPM). FutureTPM will provide a new generation of TPM-based solutions, including hardware, software and virtualization environments, by 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, Trusted Execution Environments, Smart Cards, and the Internet of Things.

Motivation

With the emergence of the Internet of Things (IoT), industry's digital transformation has begun by bringing new challenges. Security, in particular, is one of the main concerns due, in part, to recent developments in **quantum computing.** A quantum computer is different from common digital computers, where data are encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1). Instead, a quantum computation uses quantum bits (qubits), which can be in superpositions of states. Experts believe that once a fault-tolerant universal quantum computer is available, which may still be several years away, it will be capable of solving complex mathematical problems, rendering all currently used public-key cryptographic solutions insecure. As a result, the need to find ways to incorporate quantum-resistant (QR) cryptographic algorithms into "secure by design" deployed systems is becoming necessary and urgent.

FutureTPM Vision

FutureTPM will provide a **new generation of TPM-based solutions,** incorporating robust and formally verified QR cryptographic primitives. The goal is to enable a smooth transition from current TPM environments, based on existing widely used and standardised cryptographic techniques, to systems providing enhanced security through QR cryptographic functions, including secure authentication, encryption and signing functions. By designing an innovative portfolio of high-security QR algorithms for primitives such as **Key Agreement**, **Encryption**, **Signature**, **Cryptographic Hashing**, **Message Authentication Code (MAC) Functions**, and **Direct Anonymous Attestation (DAA)**, FutureTPM will fill the gaps that currently threaten its long-term security properties. This will enable FutureTPM systems to generate a secure root of trust that can be used for interacting with Cloud services, accessing corporate services, performing banking and eCommerce transactions, along with a wide range of other services.

FutureTPM Use Cases

FutureTPM aims to prove and validate the applicability, usability, effectiveness and value of the QR TPM concepts, models and algorithms in real-world settings, including industry and commerce, which may be affected by the advent of quantum computing. This will be achieved by examining their application to the following predefined set of use cases:

Online banking

To isolate the e-payment process in a more protected context so as to provide enhanced security levels against unintentional data leakage and malicious apps

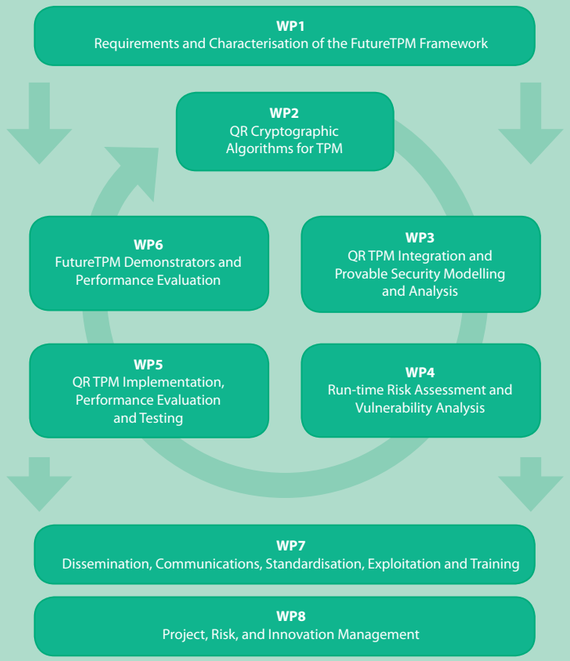
Activity tracking

To increase the trust of users of cloud-based activity tracking services in the security and privacy properties of their stored and utilised data

Device management

To help protect private keys stored on routers, mobile devices, and IoT devices against compromise or misuse by malicious applications

FutureTPM



FutureTPM Main Goals

Secure Quantum-Resistant Cryptographic Algorithms for the TPM

FutureTPM aims to identify, design and develop QR algorithms for each cryptographic primitive supported by a TPM. This includes the development of bespoke provable-secure quantum-resistant algorithms for (i) **Symmetric Cryptography**, (ii) **Asymmetric Cryptography** and (iii) **Privacy-protecting primitives**, such as **Direct Anonymous Attestation**.

Design Validation using Formal Security Analysis

FutureTPM aims to define and design appropriate **formal methods**, including computer-aided proof systems and automated proof tools, to support the security analysis model needed to reason about systems on the scale of the TPM specification. For example, the key hierarchy feature used by TPMs to store key material and other sensitive information in "untrusted" memory regions is commonly used for remotely providing key material to servers once their identity and key material has been established.

Implementation of Hardware, Software, and Virtual TPM

FutureTPM aims to demonstrate the applicability of the identified QR algorithms to the full range of possible TPM environments. This entails the implementation and rigorous evaluation of the designed QR algorithm suite in three types of TPM environment: (i) the **hardware TPM** (hTPM), (ii) the **software TPM** (sTPM), and (iii) the **virtual TPM** (vTPM).

Standardization within TCG, ISO/IEC and ETSI

Planned outcomes of the project include the development of **standardisation** proposals that push the state of the art in the areas of cryptography and the TPM itself, and will involve the technical committees of the relevant standards bodies, notably **ISO, IEC, ETSI** and the **TCG**.

Provision of Run-Time Risk Assessment and Vulnerability Analysis Methodologies

In many cases, the operation of devices hosting the TPM may leak sensitive information (e.g., via side-channel attacks) which can be used to mount successful attacks to recover secret information. In this context, the FutureTPM will design **risk analysis methods** that target all the phases of a system's development lifecycle, including from design time to near real-time risk quantification of newly identified attacks.