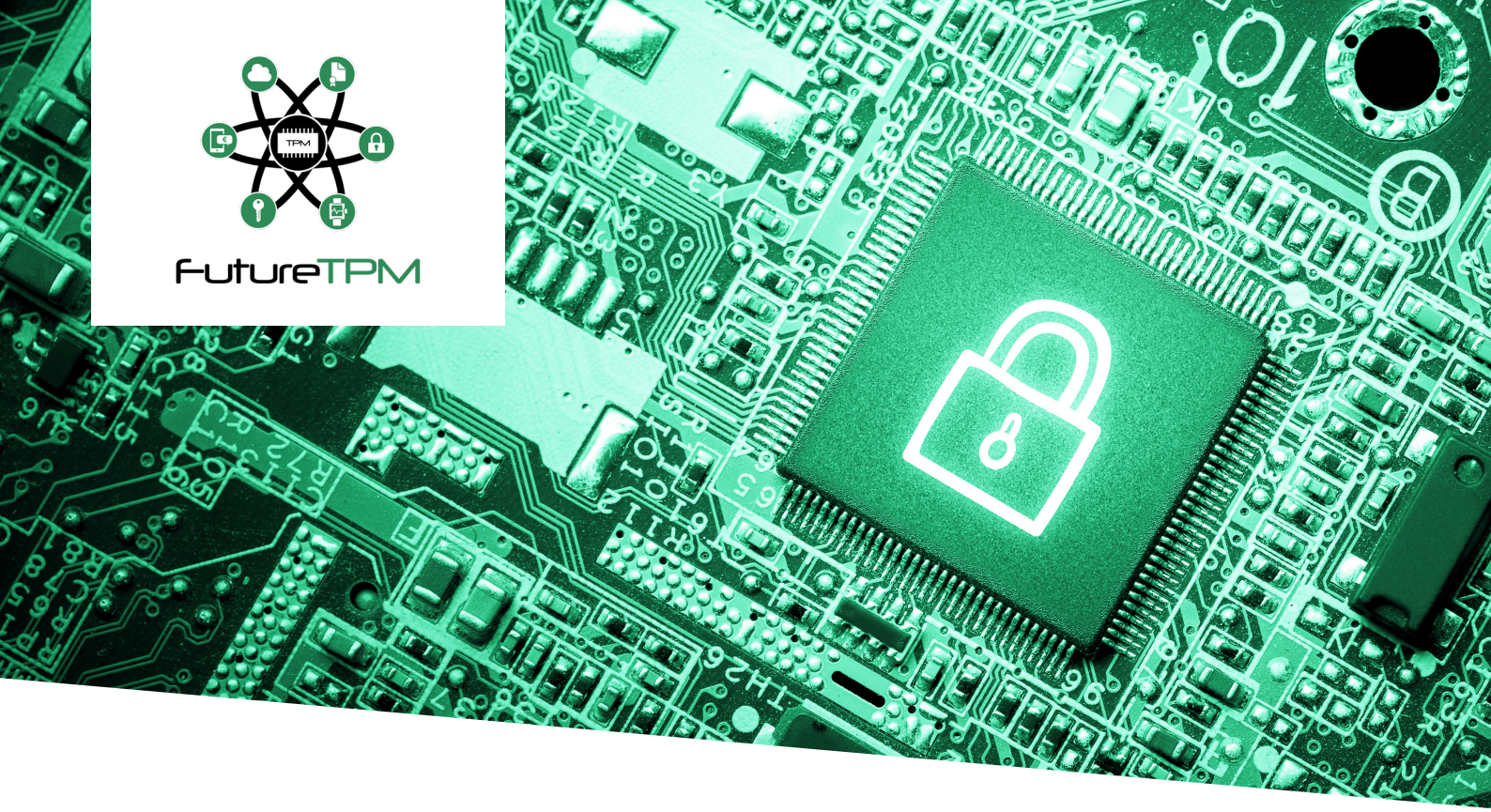


FutureTPM

Newsletter / May 2018 - Issue 1

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


**Consortium**

14 partners (8 countries)

**Project Coordinator**

MMAg.ª Martina TRUSKALLER
coordination@futuretpm.eu

**Scientific/Technical Lead**

Prof. Liqun CHEN
liqun.chen@surrey.ac.uk

Dr. Thanassis GIANNETSOS
a.giannetsos@surrey.ac.uk



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


## MAIN PROJECT INFORMATION

FutureTPM will provide a **new generation of TPM-based solutions**, incorporating robust and formally verified Quantum-Resistant (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.

### Use Cases

#### Online Banking

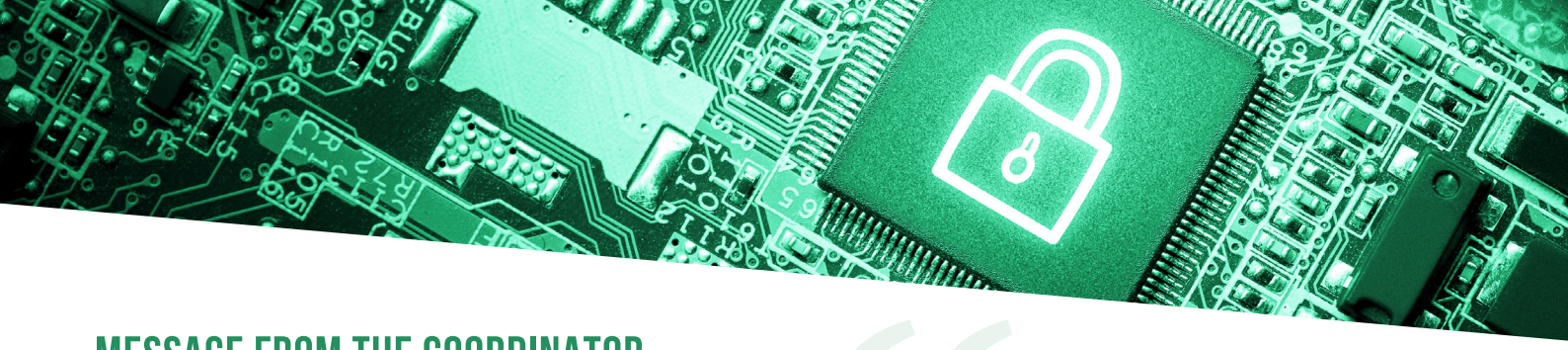
To isolate the e-payment process in a more protected context so as to provide enhanced security levels against unintentional data leakage and malicious apps

#### Activity Tracking

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

#### Device Management

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



## MESSAGE FROM THE COORDINATOR

***The intention of this newsletter is to open a new communication channel in order to provide news on the project progress and to discuss ongoing topics relevant to FutureTPM for internal and external project partners, stakeholders and all other interested bodies.***

For more detailed information about and around the project we warmly invite you to have a look on our project website, which is constantly kept up-to-date with the latest project related news: futuretpm.eu

The project has successfully started with the kick-off meeting in January 2018 and and since then the project has been progressing towards the definition of the technical and security requirements of the next-generation TPMs. The first milestone will be achieved in June 2018 when the technical and security requirements will be available, to be met used by the FutureTPM framework and the use cases.

## COMMNET² SPRING SCHOOL

**26th to 28th of March 2018, Sheffield, United Kingdom**

The CommNet² spring school is a regular event targeted at PhD students which, this year, was hosted by the University of Surrey in Guildford, UK with a focus on wireless security. In his talk, Dr. Ronald Toegl of Infineon Technologies Austria AG, gave an introduction to Trusted Computing. The main technology discussed was the Trusted Platform Module, with topics of channel vs. device security, TPM features, core concepts like the chain of trust and the applicability in network computing settings.

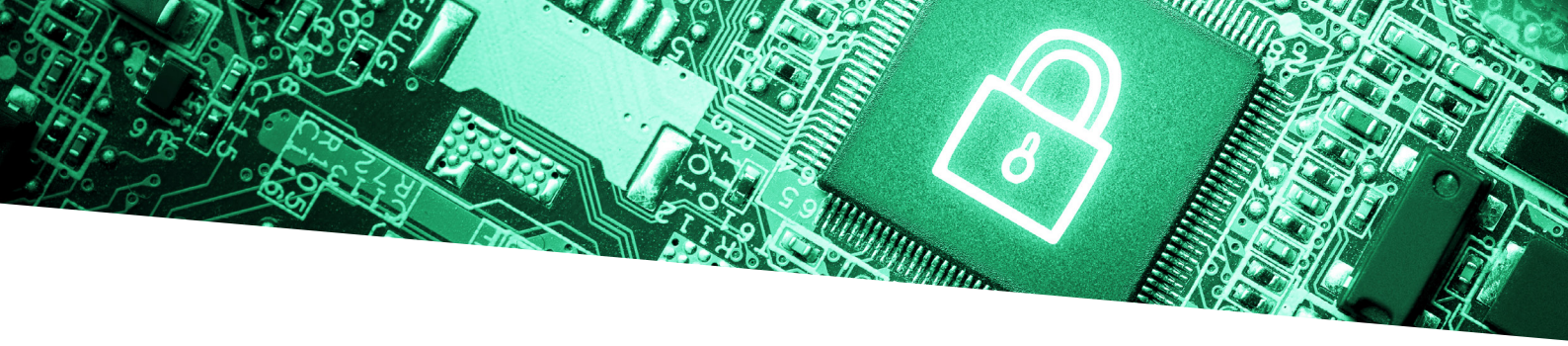
Furthermore, Dr. Thanassis Giannetsos from the Department of Computer Science, Surrey University, presented the main security and privacy challenges in IoT Edge Computing, focusing on the core edge devices, i.e., sensors, vehicles and mobile phones. He described how the use of trusted computing technologies (especially TPMs) can be used towards establishing and managing trust between entities, starting from bi-lateral interaction between two single system components and continuing as such systems get connected to ever larger entities.

## KICK-OFF MEETING

From 23rd to 24th January 2018 the FutureTPM consortium met for the kick-off meeting in Graz, Austria, at IFAT premises. The first day was dedicated to get to know each other and to organize the further collaboration of the project partners.

Afterwards the technical roadmap and key enabling technologies were discussed and a workshop on requirements and use cases was executed.

Discussions and socializing continued during a common dinner in a less formal atmosphere. The second day focused on technical discussions and agreements on the next steps in the project. Summing up, it was a very interesting and engaging meeting, providing many inputs that can be used for further research and development within the FutureTPM project.



## TECHNICAL APPROACH

The FutureTPM consortium started working on FutureTPM System Requirements and the envisioned Use Cases. The focus has been on:
(i) Identifying technical, functional and security requirements and properties of a QR tamper-resistant TPM,
(ii) refining the requirements and properties specific to the three types of TPM environment, namely software-based, hardware-based and virtualization environment, and
(iii) applying the requirements and properties to the FutureTPM use cases.
In conjunction with research partners, the use case partners have made progress in shaping their use case requirements from narrative user stories into technical requirements.
In addition to that, the consortium started to individuate possible quantum-resistant constructions for the TPM, and the possible security scenarios depending on the computational capabilities of the adversary (i.e., whether the adversary has access to a quantum computer).

## NEWS

FutureTPM arranged a cooperation call with the **H2020 PROMETHEUS** project to discuss common dissemination activities and knowledge transfer.

Participation to a panel session of post-quantum crypto at **CSIT's Annual Cyber Security Summit** which is taking place on 9-10 May 2018. Under the SAFECrypto project, Prof. Maire O'Neill is hosting a panel session on "Quantum-safe cryptography: a new era for information security" and David Galindo from University of Birmingham will present the FutureTPM project.

An application was submitted for establishing a liaison with the ISO/IEC JTC 1/SC 27 WG 2 and a call has already been set up for exploring the possibility of a liaison with the Trusted Computing Group (TCG).

Follow FutureTPM on:

**futuretpm.eu**

## SUBMITTED PUBLIC DELIVERABLES

- **D7.1** Internal and external IT communication infrastructure and project website
- **D8.1** Project quality plan

## UPCOMING PUBLIC DELIVERABLES

Public RTD Deliverables published on FutureTPM

- **D1.1** FutureTPM Use Case and System Requirements
- **D1.2** FutureTPM Reference Architecture
- **D1.3** Security Risks in QR Deployments
- **D2.1** First Report on New QR Cryptographic Primitives
- **D3.1** First Report on Security Models for the TPM

## CONFERENCES AND MEETINGS

**Cyberwatching.eu - 26th of April 2018**
@ Brussels Belgium
www.cyberwatching.eu

**University of Luxembourg Partnership Day 2018 - 5th of June 2018**
@ Luxembourg Luxembourg
wwwfr.uni.lu

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