Publishable Summary

Project number:	610436
Project acronym:	MATTHEW
Project title:	MATTHEW: Multi-entity-security using active Transmission Technology for improved Handling of Exportable security credentials Without privacy restrictions
Start date of the project:	1st November, 2013
Duration:	36 months
Programme:	FP7-ICT-2013-10

Date of the reference Annex I:	September 2016 (V1.1)
Periodic Report	Publishable Summary (as part of D7.6 3rd Periodic Report)
Period covered	1st Nov. 2015 (M25) – 31st Oct. 2016 (M36)
Deliverable reference number:	ICT-610436 / D7.6/ FINAL | 1.1
Work package contributing to the deliverable:	WP 7 (contributions of all work packages)
Due date:	October 2016 – M36
Actual submission date:	27th January, 2017

Project Coordinator	Holger Bock Infineon Technology Austria (IFAT)
Tel:	+43 51777 5393
Fax:	+43 4242 3020 5393
Email:	Holger.bock@infineon.com
Project website	www.matthew-project.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 610436

Chapter 1 Publishable Summary

Project name: **MATTHEW** *Grant Agreement*: **610436**
Start date: 1st November 2013 *Duration***:** 36 months
Project website: http://www.matthew-project.eu/
Contact: support@matthew-project.eu

Mission of MATTHEW: *The mission of the MATTHEW project is to enable new applications and services on mobile devices. It will overcome the limitation of current passive NFC transmission technologies by active modulation and offer new ways of exchanging roles from one secure entity like a nanoSIM or a microSD™ card to another with novel security and privacy approaches.*

The MATTHEW Consortium: The consortium comprises 8 partners from 4 different countries: reputable universities and recognised companies from different European Union member states (Austria, Germany, France, and Czech Republic). All partners are experts in their field. This partnership of experienced professionals is anticipated to result in a successful project.

Motivation of the MATTHEW project: With the increasingly pervasive use in our society of mobile devices like smart phones and tablets, and many users running several security relevant applications on these devices at the same time, security and privacy challenges outranging those on personal computers arise. In the near future, users are expected to move personal roles and identities between secure entities. Electronic representations of rights associated with such roles will be mobilised and reside on multiple devices.

Secure entities can be:

- a secure element (SE) integrated in a nanoSIM used in smartphones or
- a SE integrated in a wearable device[1]

Since these entities are bound to a singular user, they contain privacy sensitive data. The type of data depends on the application that these security entities are used for. In order to ensure the privacy of the user, MATTHEW investigates privacy-enhancing technologies and how to integrate them into the "multiple roots of trust"-concept in a way that the exchanged privacy-relevant information is reduced to an absolute minimum. Furthermore, this approach ensures that no sensitive data remains in a device after the secure entity has been unplugged.

Objectives & Overall Strategy: Within the framework of the MATTHEW project we focus on:

- the development of novel, privacy-preserving security applications with
- anonymity and Attribute Based Credentials (ABC);
- transferable ABC over various mobile devices like smart phones and tablets using Near Field Communication

Introducing active transmission technology for NFC, MATTHEW will overcome the greatest obstacles in scalability of form factors for NFC antennas, thus facilitating integration of NFC-enabled security components in mobile devices. MATTHEW directly addresses "security and privacy in mobile

[1] The form factor originally targeted was a SE integrated in a microSD™ card used in tablets, but this form factor was revised during the runtime of the project and SE in wearables were targeted instead

services" of the objective ICT-2013.1.5 Trustworthy ICT (Information and Communication Technologies) of the 7th framework program of the European Union and will, based on application requirements, specify an architecture with focus on multiple entity security with privacy preservation.

Component development encompasses:

- secure elements with physically unclonable functions (PUFs)
- privacy algorithms support
- active transmission technology
- antenna designs
- specialised packages for small form factor integration

Organisation of work: The work performed in the framework of this project is organised into seven different work packages with significant dependencies and expected synergies between them.

WP1 System Requirements, Architecture and Specification is responsible for deriving the requirements from a variety of target applications for the whole mobile system. Based on the findings an architecture description is developed.

WP2 Multiple Entity Security develops foundations to integrate a flexible and portable root-of-trust that represents an electronic identity of the user.

WP3 Component Hardware Development provides all the necessary hardware components, such as secure elements, transmitters and receiver components for active transmission, as well as specially miniaturised antennas.

WP4 Application Development is responsible for the physical access control use cases, the payment by phone use case and privacy preserving technologies.

WP5 Integration, Prototyping integrates all components into a very small form factor like SiP for wearable devices or nanoSIM[2]. Further prototypes will demonstrate the applications developed in WP4 such as payment and access control.

WP6 Evaluation and Testing carries out the analysis of the outcomes from WP2 and WP5 and in relation to the specification elaborated in WP1. Further standardisation will be an important task within this work package.

WP7 Project Management, Dissemination and Exploitation ensures the operational management and technical life of the project encompassing management components such as contractual, financial, legal, technical, administrative and ethical aspects.

Description of the work performed and results in the third project period

WP2 put the main focus for period 3 on the design of two privacy-preserving ticketing protocol variants (single-use and long-term) from attribute-based credentials (ABCs) that incorporate PUFs, research on new one-show and multi-show ABCs and research on underlying primitives such as digital signature schemes as well as research on the overall system security of mobile-platforms and the design, implementation and security of PUFs.

[2] The adaption of form factor for integration in wearables also effects WP5, were a system in package (SiP) was targeted as integration option instead of the originally targeted microSD™

WP4 finalized the application development such as user interface for the Mobile PayPass Android application, the SW development of Java application for scenarios, SIM and SAM applets and RSW04 reader and considered SW development in order to opens the way to privacy-preserving access by users to remote services from the MATTHEW platform.

WP5 adjusted industrial manufacturing processes in order to produce small form factor samples that were used in use cases demonstrators and in WP6 as well for test and evaluation activities.

WP6 evaluated the developed concepts towards the fit with international standards and verified the applications demonstrating the different use cases itself.

WP7 covered the management of the project, the interface with the European Commission and the dissemination of the results of the project towards both academia and industry.

Expected final results and their potential impact and use

Final results of the MATTHEW project will be manifold, from research results that turn over some of the basic assumptions that have been present before the start of the MATTHEW project to ready-to-exploit demonstrator solutions show-casing novel integration and application schemes

These results include:

- Simulation results as well as measurements on novel antenna concepts for smallest form factor integrations of RFID / NFC components with active transmission technology
- Technology demonstrators for nanoSIM and system-in-package (SiP) integration
- A prototype SiP for payment solutions in wearable devices
- An exploded platform as development tool for such payment solutions and wearable integration
- Prototypes for novel access control systems with mobile devices based on CIPURSE open standard protocols including novel 4-eyes principle for high-security zones
- CIPURSE SAM integration into reader device of such enhanced access control system
- Open Source library for pairing primitives implemented with special focus on embedded devices
- Group Signature as well as ABC-based protocols for privacy preserving anonymous credential validation
- Pairing implementation on embedded secure element prototype
- Ticketing demonstrator solution for single use tickets building upon one-show ABCs
- Ticketing demonstrator solution for limited time tickets building upon multi-show ABCs

All of these solutions have in common, that they are dealing with more than one secure element in context with mobile platforms.

In addition research results have been published on novel attack techniques exploitable in mobile devices underlining the need for hardware based security as trust anchors in such platforms

The potential impact of these solutions varies according to their technology readiness level. Whereas the payment and access control solutions may be exploited more or less straight forward in their respective markets, the anonymity and privacy preserving solutions are serving as demonstrators to show-case what is possible already today with pairing based cryptography on mobile platforms, since such efficient privacy preserving schemes have not been available before the MATTHEW project.