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:	1st November 2013
Periodic Report	2nd Periodic Report
Period covered	1st Nov. 2014 (M13) – 31st Oct. 2015 (M24)
Deliverable reference number:	ICT-610436 / D7.5/ FINAL | 1.1
Work package contributing to the deliverable:	WP 7 (contributions of all work packages)
Due date:	October 2015 – M24
Actual submission date:	29.02.2016, V1.1

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 microSD™ card used in tablets

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 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 microSD™. 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 second project period

The MATTHEW project started in November 2013 and is set to run for 36 months. During the second project phase, corresponding to the second project year, the focus was placed on system security by utilizing pairing based privacy preserving protocols like group signature schemes and ABCs, PUFs and multiple SEs, antenna design and its hardware development as well as the integration of a nanoSIM prototype, the development of the corresponding application software as well as standardization. WP1 successfully ended with positive outcome that further influenced development of the remaining WP´s. Throughout the second project period, five deliverables were submitted and one milestone was reached.

WP02 (Multiple Entity Security) started immediately with the project start in month M01, i.e., in November 2013, together with WP1. Right from the start, the discussion on scenarios for the use of mobile platforms with multiple secure elements has been a central element in all meetings. During the run of those discussions it was agreed amongst the MATTHEW consortium partners that – as an extension to the use cases mentioned in the DoW – a **third use case** (UC3) building a **ticketing scenario** should be established in the research area of transfer of credentials in a privacy enhanced protocol environment.

The privacy enhancing technology chosen for this use case is the class of group signature schemes, allowing for (zero knowledge) proofs about the knowledge of an individual secret and the membership of a group without revealing the individual identity of the secret owner/holder. Consequently, the definition of the use case involving multiple secure elements to ensure the requirements were captured and included in platform requirements D1.1.

Already within the first year, a first **draft** for such an **anonymous ticketing protocol** based on group signatures was made. The final protocol allows a user to download single-use as well as long-term tickets and present them anonymously when accessing the transport system (e.g., Metro or bus). Verification is performed locally by the terminal (e.g., NFC reader) and validates the authenticity of the ticket without being able to link it to the ticket issuance process, even in front of colluding issuers and verifiers. These ticketing protocols have then been further extended, i.e., **revocation of long-term tickets** and **transferability of single-use tickets** have been taken into account. The final group-signature-based ticketing protocol taking PUFs and the efficiency and security of implementations into account has been delivered in D2.1.

Additionally, **six papers** with MATTHEW affiliation have already been **published** in year one and **another six papers** in the second year. Nine out of these twelve papers give a practical insight into the implementation security requirements of required cryptographic base primitives such as hash functions, ciphers, elliptic curves and cryptographic pairings, their impact on performance, and their vulnerability to several types of implementation attacks. The remaining papers deal with privacy-enhancing cryptography: with one-show and multi-show ABCs and their base primitives such as different types of digital signature schemes (structure-preserving signatures and blind signatures).

Three frameworks have been developed and been made publicly available as **open source**: one elliptic curve cryptography C library, one bilinear pairing C library and one framework for computing the ECDLP. In parallel, different pairing libraries have been evaluated and progress has been made towards implementing ABC-based protocols on security controllers. Furthermore, **RO-PUFs** have been implemented, the implementation has been evaluated and helper-data algorithms have been designed for the implementation.

WP03 (Component Hardware Development) activities have been very challenging for all project members (like all other WPs in the Matthew project) and during execution of their tasks WP3 members did face several deep technical challenges that were successfully overcome. As well during the technical work the WP members did proactively look at the market and were able to identify also new markets trend (high demand of wearable device implementing core Matthew project functionality) that have been translated into new technical requirements. An additional use case with an ad-hoc demonstrator system architecture targeted to wearable market have been defined and the HW implementation did start. The work towards ATT-HW did achieve all internal milestones, despite a small delay that was faced during the design phase of analog / digital blocks (well tracked in the risk assessment), and the ATT-HW test silicon was successfully taped out in August and first samples have been made available to partners in October. The work towards the first nanoSIM prototype implementation that included Electromagnetic system simulation and nanoSIM demonstrator engineering did proceed during the reporting period by respecting all milestone and partner were able to finalize the nanoSIM package configuration with success and transfer the design data to outsourcing partners for manufacturing. To conclude we are satisfied of the work done in the WP3 and we achieved all milestone.

WP04 (Application Development) focuses on application development linked to three main use cases that exemplify the technologies enabled by the MATTHEW platform: Payment by phone using the phone's microSD™ slot (Gemalto), physical access control (partner IMA), and Privacy-preserving access to remote services (CRX). The first use case will describe how to perform a payment transaction at least as securely as would be achieved using a traditional contactless smart Card. The application will be developed in order to study its ergonomic aspects, performances and security in

the EMV context. The payment use case has been reoriented by Gemalto in the 2nd year, with the approbation of MATTHEW partners, to address wearable device market. The Access control use case includes three scenarios and intends to show how the improved security brought by the new NFC technology can be used by developing the new applications described in the Task 4.2. New applications designed and developed in this work package will prove a benefit in terms of increased efficiency and robustness of the NFC services security implemented in Access control systems. The third use case opens the way to privacy-preserving access by users to remote services from the MATTHEW platform. Although the core software (a cryptographic API supporting an ABC system) is intended to be fully generic towards the nature of the remote service, the prototype will select a specific case for demonstration purposes. The objective in 2nd period has been re-oriented to a new target output consisting of a demonstrator for a ticketing application on an Android mobile phone.

The initial target of **WP05 (Integration, Prototyping)** consisting in the integration of a secure platform, embedding the different components developed by the consortium, inside a microSD card form factor, has been reoriented to follow the new orientations of the mobile payment market evolution. Indeed, the market analysis, realized by the consortium, identified that mobile device manufacturers, with the deployment of cloud based storage, address their design and integration constraints by removing the microSD interface and improving their Bluetooth Low Energy (BLE) connectivity in their equipment, as already done by Apple in the iPhone and recently by Samsung as well in their last high runner handsets. For these reasons, the integration effort performed in WP5 has been reoriented to address the new "wearable" fast growing market segment, whose ergonomic and use cases match the final objectives of the MATTHEW project with respect to transferability, as replacing the connecting interface from the secure element to the mobile platform by a Bluetooth type connection instead of the microSD interface, the secure element may be transferred from one mobile to another one by disconnecting and re-connecting via BLE instead of unplugging and re-plugging the microSD card.

At this time, the consortium defined in details the final form factor and the internal architecture of a "Solution In Package" (SiP) component that could be integrated in future wearable objects in order to upgrade their device with new secure contactless applications. Thanks to their BLE connectivity, connected devices will be able to interact with, and offer the SiP services to remote mobile equipments like handsets or tablets .The design of the SiP component has been particularly cared to reduce as much as possible the footprint on board to respond to manufacturer integration constraints.

In **WP06 (Evaluation and Testing)** of the MATTHEW project main focus of activities has been seen on standardisation work, scheduled in task T6.3 – "Standardisation Activities", since tasks T6.1 – "Contactless Verification" and T6.2 "Application testing and evaluation" are scheduled for the third year, starting in project months M28 and M30, respectively. MATTHEW partners were preparing their contributions to standardisation by extensive in-house studies and measurements to provide profound input at the standardisation meetings. Examples for standardisation bodies in which MATTHEW partners are directly participating or contributing through their national bodies (AFNOR, DIN, ASI) and representatives are:

- ISO ISO/IEC JTC 1/SC 17/WG 08 "Integrated circuit cards without contacts" including its TF2
- ISO/IEC 20008-2 "Anonymous signatures: Mechanisms based on a Group Key"
- new ISO standard to be created on ABCs within SC 27 WG5
- ETSI SCP TEST44, TEST45 and TEC57

By these contributions MATTHEW partners are driving standardisation for new cryptographic standards as well as contactless active transmission technologies.

WP07 (Project Management, Dissemination and Exploitation) was responsible for the effective organisation of the project and covered all relevant management components as well as for the

dissemination of project results. Some of the main achievements so far have been: the organization of meetings (e.g. Technical and GA Meetings), monitoring of the work plan (Interim Management Reporting) and supporting partners in everyday issues. The robust IT infrastructure (website, SVN repository including web access, mailing lists including mailing list archives) is regularly updated. Several dissemination activities to raise the awareness (poster, project flyer, poster presentations, etc.) of the MATTHEW project have been performed, several scientific articles have been submitted and a couple of presentations were given. Stakeholders of the MATTHEW project are regularly informed about upcoming dissemination activities, project meetings as well as further achievements on Twitter as well as on the MATTHEW project website http://www.matthew-project.eu/ including a project blog.

Expected final results and their potential impact and use

The expected final results of the MATTHEW-project are two-fold: On the one hand the consortium expects fully functional use case demonstrators of the 3 use-cases, a contactless payment application with active enhanced transmission technology, an NFC access control application implementing a 4-eyes principle based on a secure protocol involving 3 secure elements, and a privacy preserving electronic ticketing use-case with transferable credentials. Despite the fact that those three use cases have different technology readiness levels, all will profit directly from the research results on hardware-and software component level performed during the project.

On the other hand novel concepts and protocols are expected that shall stimulate further research in the area of future mobile platforms with multiple secure elements, also – but not limited to – environments with increased privacy considerations. All those results will be supported by an underlying technology innovation for mobile platforms, which is an enhanced active transmission technology, overcoming communications limitations as they had to be faced, before the MATTHEW project was in place. In addition this innovation shall support further miniaturization and support smallest form factors like nanoSIM.