# 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** | Publishable Summary<br>(as part of D7.4 "1st periodic report according to EC regulations of the model contract") |
| **Period covered** | 1st Nov. 2013 (M01) – 31st Oct. 2014 (M12) |
| **Deliverable reference number:** | ICT-610436 / D7.4/ FINAL \| 1.0 |
| **Activity and Work package contributing to the deliverable:** | WP 7 (contributions of all work packages) |
| **Due date:** | October 2014 – M12 |
| **Actual submission date:** | 23.12.2014, V1.0 |



| | |
|---|---|
| **Project Coordinator** | Holger Bock<br>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 first project period

The MATTHEW project started in November 2013 and is set to run for 36 months. During the first project phase, corresponding to the first project year, the focus was placed on the MATTHEW system specification and requirements. All work packages, apart from WP 5 (starts in M18) that has not yet started, initiated work and produced altogether 4 deliverables (including this first Periodic Report) throughout the first project year.

**WP01 (System Requirements, Architecture and Specification)** of the MATTHEW project started immediately with the project start in month M01, i.e. in November 2013. On the one hand this work package laid the foundations for the whole project by collecting and analysing the use case requirements derived from three very different use cases. These use cases included a mobile payment application with offline transaction in two different variants supported by active transmission technology, a four-eye-principle based access control scenario for high security areas and an advanced, privacy-enhanced ticketing use case with the demand for transferable credentials. The results of these investigations on use case requirements were documented in D1.1 “Report on use case and system architecture requirements”, which was due in month M05, i.e. March 2014 and finalized in time. On the other hand the collaborative work of the project partners resulted in a specification document defining the overall architecture of the MATTHEW system based on a role

model showing the architecture elements which are common to all the three use cases. The respective deliverable has the title “Report on MATTHEW Platform Specifications” and describes the MATTHEW platform architecture with its components and interfaces highlighting the sub-components on which research and implementation will be focused during the following periods in the project. It includes the description of the MATTHEW demonstrators and how they are derived and tailored from the overall architecture. The D1.2 was due in month M10, i.e. August 2014 and was delivered in time. Thus the milestone MS1 – “Use case and system architecture specified” could be achieved in time in month M10 and the work package W01 of the MATTHEW project could be closed as planned.

**WP02 (Multiple Entity Security)** of the MATTHEW project 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 are 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 protocol allows a user to download a single-use ticket and spend it 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 ticket issuance, even when the verifier and the issuer collude. Additionally, **six papers** with MATTHEW affiliation have already been **published**. These papers give a practical insight into the implementation security requirements of cryptographic pairings, their impact on performance, and their vulnerability to several types of implementation attacks.

**WP03 (Component Hardware Development)** of the Matthew project started in month M06 (i.e. May 2014) immediately after D1.1 (first report of WP1 that define system architecture requirements and use cases). The definition of an innovative and improved concept for active transmission technology together with a new antenna concept that allow its miniaturization and integration into very small devices like µSD and SIM card has been topic of discussion during all meetings. Together with active transmission technology and antenna topology was also discussed the best interface configuration between radio front-end and secure element in order to allow interoperability with traditional secure element designed to operate with passive card and at the same time enable new generation of secure element with additional feature and re-configuration capabilities via active transmission technology based radio font-end. Outcome of studies and defined requirements brought us to the definition of a complete architecture for a new generation of active transmission technology based front-end plus the definition of a new antenna concept that will allow easy integration in existing µSD and SIM packages.

**WP04 (Application Development)** has been scheduled to begin on M08. All below work activities followed the requirements collection process and application specification done in WP1. This work package shall develop applications for three main use cases that exemplify the technologies enabled by the MATTHEW platform: Application for advanced mobile payment, Application for physical access control and application for advanced anonymous ticketing. All involved partners declared the WP summary defined in the DoW is still in line with current targets Software architecture for mobile payment application has been described and development of Android microSD service has started. On the application for physical AC, the activity in the first period aimed to identify and describe all IDSIMA4 modules affected by further development. Preparatory work on advanced ticketing

application development reflected the activity in WP2 focused on anonymous ticketing protocol, security implementation and use of the PUF.

**WP06 (Evaluation and Testing)** is fully in line with the project plan, task T6.3 – standardization activities – having started in M01 of the MATTHEW project, the other tasks, T6.1 and T6.2 waiting to be started during the third reporting period in the months M28 and M30, respectively. Preparative actions for task T6.2 like ordering and purchase of equipment have been triggered by the respective partners.

**WP07 (Project Management, Dissemination and Exploitation)** was responsible for the effective organization of the project and covered all relevant management components. Some of the main achievements so far have been: the organization of meetings (e.g. Kick-Off and GA Meeting), the implementation of monthly EB Telcos, monitoring of the work plan (Interim Management Reporting), supporting partners in everyday issues (handling day2day requests), etc. Further a robust IT infrastructure (web site, SVN repository including web access, mailing lists including mailing list archives) was established and regularly updated since. A list of dissemination activities has been compiled and updated periodically, where scientific publications, participation in conferences and other activities to ensure the visibility of the project, are listed.

**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-eyey 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.