Multi-entity-security using active Transmission Technology for improved Handling of Exportable security credentials without privacy restrictions

Project number:	**610436**
Project website:	**www.matthew-project.eu**
Project start:	**1 November, 2013**
Project duration:	**3 years**
Total costs:	**EUR 5.972.553,-**
EC contribution:	**EUR 3.600.000,-**

MATTHEW is co-funded by the European Union under EU Framework Programme 7

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 mobile platform like a smartphone or tablet to another.

Motivation:

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 as used in smartphones or tablets can be:

- a secure element (SE) integrated in a nanoSIM used in smartphones or
- a SE integrated in a microSD™ card used in tablets or
- a SE embedded in the mobile platform

Since these entities are bound to a single 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 a minimum. Furthermore, this approach ensures that no sensitive data remains in a device after the secure entity has been unplugged.

Objectives:

Within the framework of the MATTHEW project we focus on:

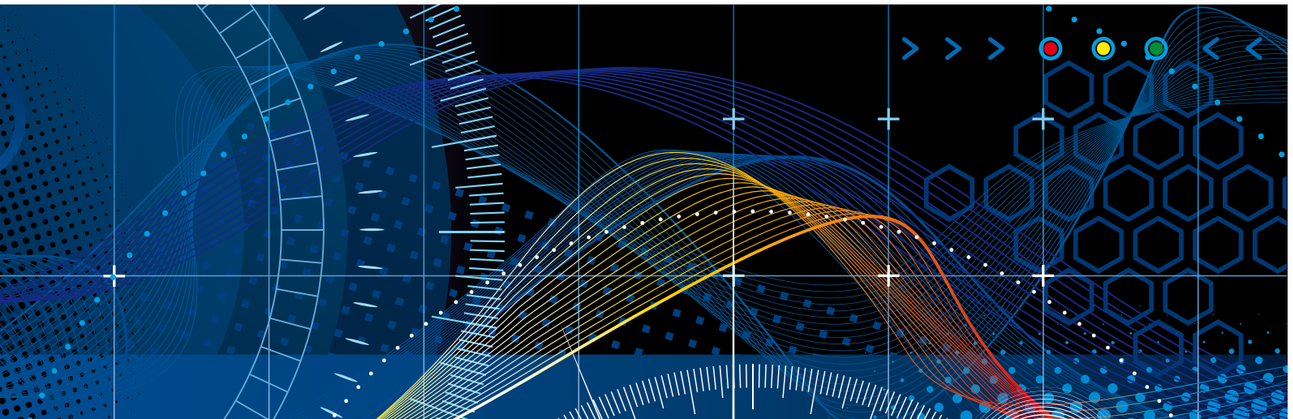
- the development of novel, privacy-preserving security applications with
- anonymity and Attribute Based Credentials (ABC) or group signatures;
- transferable Credentials over various mobile devices like smartphones and tablets using Near Field Communication (NFC)

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.

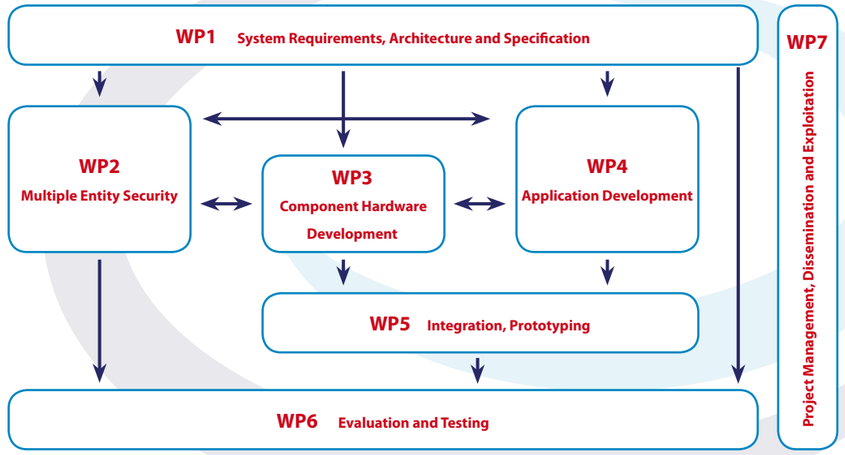
Component development encompasses

- privacy algorithms support
- active transmission technology
- antenna designs
- specialised packages for small form factor integration



matthew

Project Overview:



Work Packages:

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
Work package 1 is dedicated to 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
In work package 2 the foundations to integrate a flexible and portable root-of-trust that represents an electronic identity of the user will be developed.

WP3 Component Hardware Development
In work package 3 all the necessary hardware components will be provided, such as secure elements, transmitters and receiver components for active transmission, as well as specially miniaturised antennas.

WP4 Application Development
This work package is dedicated to the physical access control use cases, the payment by phone use case and privacy preserving technologies.

WP5 Integration, Prototyping
In work package 5 all components will be integrated into a very small form factor like microSDTM. Further prototypes will demonstrate the applications developed in WP4 such as payment and access control.

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

WP7 Project Management, Dissemination and Exploitation
Finally, in work package 7 the operational management and technical life of the project encompassing management components such as contractual, financial, legal, technical, administrative and ethical aspects will be ensured.

Project Results:

MATTHEW results will be demonstrated by:

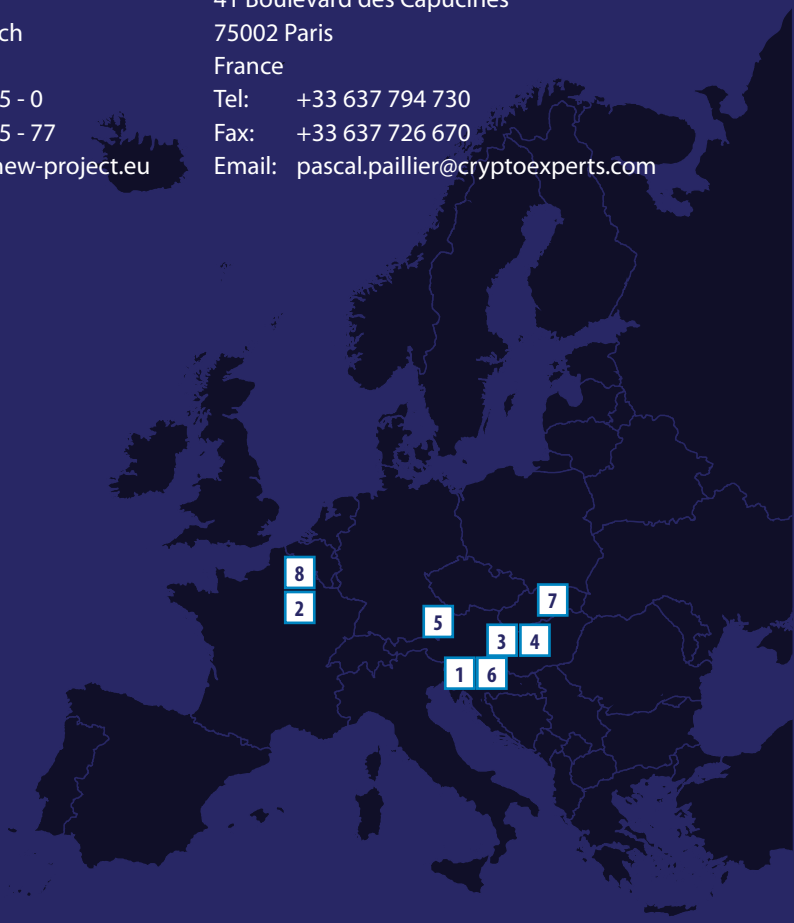
- a transferable payment application and
- multi-key access control system and
- a group signature or ABC-based cryptographic API (Application Programming Interface) will provide pseudonyms for privacy.

Contact:

Project Coordinator
Dipl. Ing. Holger Bock
Infineon Technologies Austria AG
Siemensstraße 2
9500 Villach
Austria
Tel: + 43 51777 5393
Fax: +43 4242 3020 5393
Email: holger.bock@infineon.com

Administrative Supporter
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungs-
gesellschaft mbH
Burgplatz 3a, 9500 Villach
Austria
Tel.: +43 4242 233 55 - 0
Fax: +43 4242 233 55 - 77
Email: support@matthew-project.eu

Scientific Leader
Dr. Pascal Paillier
Cryptoexperts
41 Boulevard des Capucines
75002 Paris
France
Tel: +33 637 794 730
Fax: +33 637 726 670
Email: pascal.paillier@cryptoexperts.com



Consortium:

The MATTHEW consortium is well-positioned to achieve its objectives by bringing together a team of leading industrial and research companies, research-oriented SMEs as well as well respected European universities. These 8 project partners from 4 different countries form a complete chain stretching from basic research and service design, via applied research, up to end-user oriented service providers.

1 **Infineon Technologies Austria AG (Villach/Austria)**

2 **Gemalto SA (Meudon/France)**

3 **AMS AG (Unterpremstaetten/Austria)**

4 **Graz University of Technology (Graz/Austria)**

5 **Infineon Technologies AG (Neubiberg/Germany)**

6 **Technikon Forschungs- und Planungsgesellschaft mbH (Villach/Austria)**

7 **Institute of Microelectronic Applications Ltd. (Prague/Czech Republic)**

8 **Cryptoexperts (Paris/France)**