Announcement Letter

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

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 multiple mobile 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 mobile platforms. Electronic representations of rights associated with such roles will be mobilized and reside on multiple devices.

Secure entities as used in smart phones or tablets can be:

- a secure element (SE) integrated in a nanoSIM used in smart phones or
- a SE integrated in a microSD™ card use in tablets

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.

The objectives of MATTHEW are

- 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 tables using Near Field Communication (NFC)

Introducing active transmission technology for NFC, MATTHEW will overcome the heaviest 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) 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
- specialized packages for small form factor integration

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 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. The MATTHEW partners are:

- Infineon Technologies Austria AG, Austria
- Gemalto SA, France
- AMS AG, Austria
- Technische Universität Graz, Austria
- Infineon Technologies AG, Germany
- Technikon Forschungs- und Planungsgesellschaft mbH, Austria
- Institut Mikroelektronickych Aplikaci S.R.O., Czech Republic
- Cryptoexperts, France

The MATTHEW project has started on 1st November 2013 with a set duration of 36 months. It has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 610436.

For more information visit the official MATTHEW project website: http://www.matthew-project.eu.

Contact information:

Project Coordinator
Dipl. Ing. Holger Bock

Infineon Technologies
Austria AG
Siemensstraße 2
9500 Villach
Austria
Email: holger.bock@infineon.com

Administrative Support
Dr. Klaus-Michael Koch

TECHNIKON
Forschungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Email: support@matthew-project.eu

Scientific Lead
Dr. Pascal Paillier

Cryptoexperts
41 Boulevard des Capucines
75002 Paris
France

Email: pascal.paillier@cryptoexperts.com