Press Release

Increased data protection for consumers in contactless ticketing systems: Infineon-led research project concluded successfully.

Joint press information from the partners in the European research project **“**MATTHEW”

Graz, May 23rd 2017 – Contactless technologies are increasingly shaping our everyday life, and there are millions in use worldwide. Examples include season tickets for local public transport and company identity cards for secure access control. Near Field Communication (NFC) ensures that payments at cash desks are fast and convenient with contactless bank cards, by smartphone or using smart wearables, such as an NFC-enabled wristwatch. The European research project “Multi-entity-security using Active Transmission Technology for improved Handling of Exportable security credentials Without privacy restrictions” (MATTHEW) has now developed these contactless technologies further. The use of new encryption processes is providing consumers with enhanced data protection in smart card systems. In addition, the hardware-based security solutions used in NFC applications, such as secure payment and access control, are enabling more stable communication connections and smaller form factors. The efficiency of the security solutions developed by MATTHEW has been successfully demonstrated in these three selected areas of application.

The project, which was coordinated by Infineon Technologies Austria, was successfully concluded with a review in Brussels. MATTHEW started in November 2013 and ran for a term of 36 months. Eight technology partners took part in total, from four European countries. The total budget was almost € 6 million, of which € 3.6 million was funded by the 7th EU Framework Programme.

Anonymous tickets: complex algorithms on microcomputers

One focus of the research project was on the development of cryptographic algorithms for smart card systems to protect consumers’ privacy. These can be used for example in local public transport tickets to effectively prevent electronic tracking of the respective users. A large proportion of the existing ticketing systems still work with fixed serial numbers, which are deposited on the owner’s

Infineon Technologies Austria AG
Communications
Mag. Alexander Tarzi
Phone: +43 51777-2954
alexander.tarzi@infineon.com

tickets. By reconciling these electronically with the access terminal, the system operator can easily trace which route a passenger has travelled with his season ticket.

In the MATTHEW project, the traditional public key processes were replaced by an extended encryption procedure based on cryptographic pairings. Attribute-Based Credentials (ABC) were implemented on the smart cards' microcomputers. In this way only the attribute representing the respective usage entitlement is checked, for example "to use the bus in Zone X". However, each time the card is inspected the data is presented differently, so that the user's privacy is retained. This anonymised ticketing solution has been successfully demonstrated in the form of an Android app for a multizone transport system.

"Together with its partners in the European research project MATTHEW, Infineon has developed advanced security and data protection concepts to make using contactless technologies even more secure, more stable and more consumer-friendly for the users", said Stefan Rohringer, head of the Graz Development Center of Infineon Technologies Austria AG. "This research cooperation strengthens the competitiveness of the European IT security industry, and at the same time consumers' privacy is being better protected."

Hardware-based security solutions for use in smart wearables

An additional further objective of MATTHEW was to make the communication between mobile devices and payment terminals even more stable during NFC payment transactions and for access control. For this, active NFC transmission technologies were developed in which security chips were built in to an integrated system solution (system in package). In combination with an improved antenna design, this supports reliable and secure NFC communication for the smallest-sized devices. Personal entitlements can thus be transmitted to different devices by means of small replaceable units such as nano-SIM cards. Smart wearables, for example a battery-aided wristwatch, are thus independent of often insufficient close range energy supplies, and NFC transactions can be executed despite interference fields and the device being covered by a metallic environment. For contactless payment, the system-in-package integration form from Gemalto and the nano-SIM version from Infineon were tested using payment terminals corresponding to the international EMV standard. For secure access control by smartphone, a field test was undertaken at one of the development sites, using an infrastructure based on the open CIPURSE standard.

Infineon Technologies Austria AG
Communications
Mag. Alexander Tarzi
Phone: +43 51777-2954
alexander.tarzi@infineon.com

MATTHEW research partners

A total of 73 researchers were involved in the MATTHEW project, and 19 scientific works were published. The MATTHEW partners come from four European countries - Germany, France, Austria and the Czech Republic. They include ams AG, CryptoExperts SAS, Gemalto S.A., IMA s.r.o., Infineon Technologies AG (with branches in Germany and Austria), Technikon Forschungs- und Planungsgesellschaft mbH und Graz University of Technology.

About Infineon Austria

Infineon Technologies AG is a group company of Infineon Technologies AG, a leading global supplier of semiconductor solutions that make life easier, safer and greener. Microelectronics from Infineon reduce the energy consumption of consumer electronics, household appliances and industrial plants alike. Microelectronic components contribute to convenience, safety and sustainability of vehicles and enable safe transactions in a networked world.

Infineon Austria is the only site besides Germany where R & D expertise, production know-how and global business responsibility are pooled. The company headquarters are in Villach; subsidiaries are located in Graz, Klagenfurt, Linz and Vienna. In the 2016 fiscal year (ending September 30), the company reported sales of Euro 1.8 billion with more than 3,600 employees (of which 1,400 in R&D) from some 60 nations. Research expenditure of € 400+ million make Infineon Austria one of the strongest research companies in Austria.

Contact and more information

Infineon Technologies Austria AG
Mag. Alexander Tarzi
Communications
Siemensstraße 2
9500 Villach, Austria

Phone: 051777-2954
E-mail: alexander.tarzi@infineon.com

Follow us: twitter.com/Infineon - facebook.com/Infineon –plus.google.com/+Infineon