# D6.3

# Report on standardisation activities

| | |
|---|---|
| **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 |

| | |
|---|---|
| **Deliverable type:** | Report |
| **Deliverable reference number:** | ICT-610436 / D6.3/ v1.0 |
| **Activity and Work package contributing to the deliverable:** | WP 6 |
| **Due date:** | M36, October 2016 |
| **Actual submission date:** | November 1st, 2016 |

| | |
|---|---|
| **Responsible organisation:** | IFAT |
| **Editor:** | Holger Bock |
| **Dissemination level:** | Public |
| **Revision:** | FINAL \| v1.0 |

| | |
|---|---|
| **Abstract:** | Report covering standardisation activities of MATTHEW project partners on national as well as on international level during the 3 years runtime of the MATTHEW project. Focus areas are active transmission technology and privacy mechanisms based on Attribute Based Credentials (ABCs) |
| **Keywords:** | Standardisation, ISO, ETSI, NFC Forum, EMVCo, AFNOR, ASI |

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 610436.

**Editor**

Holger Bock (IFAT)

**Contributors** (ordered according to beneficiary numbers)

Josef Gruber, Josef Riegebauer, Andreas Wörle (IFAT)

Christian Dietrich, (GTO)

Giuliano Manzi, (AMS)

Pascal Paillier, Cécile Delerablée (CRX)

**Disclaimer**

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user uses the information at its sole risk and liability.

# Executive Summary

Since standardisation is seen to be one of the major success factors for world-wide uptake of research results in mass products it was clear from the beginning, that MATTHEW project partners will engage in their respective fields of interest in standardisation processes and standardisation entities on national as well as on international level. To reflect such activities in the overall MATTHEW project context a dedicated task T6.3 had been defined already in the project proposal and has been ongoing in parallel to all research activities during the complete runtime of the MATTHEW project.

This document – the deliverable D6.3 “Report on Standardisation Activities” – describes the standardisation activities performed by MATTHEW partners in the context of active transmission technologies and its related areas like ISO14443, NFC Forum, and EMVCo, as well as activities in the area of security and privacy on ISO SC27 level.

# Contents

# List of Tables

# Chapter 1 Introduction

Successful exploitation strategies for hardware security products with high volume mass-production are often going hand in hand with international standardisation procedures, to ensure mid-term and long-term stability of infrastructure investments and interoperability in the targeted eco-systems. Thus also for the uptake of the MATTHEW project results standardisation activities of the MATTHEW project consortium partners have been considered of utmost importance.

The context for the standardisation activities around MATTHEW research results was planned to be two-fold: On the one hand it should concern updates on active transmission technology as it has been researched, developed and elaborated in the MATTHEW project, on the other hand the consortium members were supposed to be focussing on security and privacy relevant standardisation streams. Active transmission results were seen to be standardized in the ISO/IEC JTC1 SC17 and described in the standards ISO/IEC 14443 and ISO/IEC 15693, whereas security and privacy relevant results of the MATTHEW project were projected to be integrated in standards like ISO sub-committee 27 (SC 27, Security Techniques), especially in its working group WG5 focusing on Identity Management and Privacy.

During the runtime of the MATTHEW project it got clear, that – especially for payment applications as they are targeted out of use case UC1 – the harmonization between EMVCo, NFC-Forum and ISO14443 standards got more and more relevance. Thus the engagement of MATTHEW consortium partners in such activities was increased and also showed positive results, although.

Since in many cases proposals to updates and/or amendments of standards can only be handed in via national standardization bodies and usually the delegation of representatives to standardisation groups is handled or at least coordinated by national institutions, the consortium members are also presented within such national groups. It is also important to have them aligned to make sure that international and national standards do not diverge or counteract each other.

This report on standardisation activities is structured as follows: First standardization activities on international level are described, both for the fields of active transmission technology and for the fields of security and privacy. After this some national activities are listed to give an impression on the contribution to standardization through national entities and their activities. In both chapters the activities are clustered according to MATTHEW consortium partners.

# Chapter 2 Standardisation on international level

Standardisation on international level is ensuring the world wide interoperability of systems, both on physical and on logical level. While specifications for RFID-like systems on protocol level can be implemented and tested very straight forward the specification of corner cases and test scenarios on physical level (energy transmission, analogue levels and frequency characteristics) are often endangered to leave some more room for interpretation. Thus it is important to send experts from industries who are experienced in implementing use cases in the field to the standardisation meetings and procedures, to ensure that infrastructures and devices making use of such infrastructures – which are being tested according to the standardised test procedures – are able to interoperate with implementations from different manufacturers, even if the tests have been performed on abstract test setups and not within the target infrastructures. For cryptographic protocols implementing security and privacy relevant functionalities the standardisation process does not only target functionality and interoperability, but also an evaluation of the proposed algorithms in terms of their ability to provide the desired asset protection qualities.

## 2.1 Standardisation for NFC and Active Transmission Technology

Although the ISO 14443 standard has been out now for many years still several adaptions had been necessary. Two such refinement cycles for the ISO standard have been ongoing during the 3 years' run time of the MATTHEW project: First the introduction of active transmission technology added a new flavour to the world of contactless communication standards that had originally been dealing with passive PICCs only. Second test methods had to be re-aligned to improve interoperability on physical layer.

In addition the harmonization of analogue parameters between the worlds of ISO, NFC Forum and EMVCo were of utmost importance, especially for the MATTHEW use case UC1 in which payment applications with active transmission technology should be further enabled and pushed to the market area of wearables.

**<u>Activities by partner IFAT</u>**

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| 30.9. – 2.10.2015 | Vienna (A) | ISO SC17 WG8 and TF2 | IFAT: Riegebauer / Gruber | Liaison with ISO TC204/CEN TC278<br>RESOLUTION 743/15 |

| | | | | |
|---|---|---|---|---|
| 19.-23.10.2015 | Vancouver (CA) | NFC Forum All Members Meeting | IFAT: Wörle/Khemani | Analog Technical Specification<br>Progress in Analog harmonization |
| 02. – 05.11.2015 | Sophia Antipolis (F) | ETSI SCP TEST46 | IFAT: Riegebauer | cross-check SWP/HCI test cases |
| 02. – 05.11.2015 | Sophia Antipolis (F) | ETSI SCP TEC60 | IFAT: Riegebauer | HCI host network<br>SWP Interface Reactivation |
| 20. – 21.01.2016 | F2F London (UK) | TC EMVCo Alignment Taskforce (NFC Forum) and L1WG (EMVCo) | IFAT: Wörle | Harmonization of Analog Parameters NFC Forum<-> EMVCo |
| 28.01.2016 | Conf call | ETSI SCP TEST47 | IFAT: Riegebauer | READ BLOCK 0 as "public" command for CLT testing |
| 04.02.2016 | Conf call | ETSI SCP TEST47 | IFAT: Riegebauer | 1st Rel-12 conformance requirements |
| 01. – 05.02.2016 | Kyoto (JP) | ISO SC17 WG8 and TF2 | IFAT: Riegebauer / Gruber | Low power class control mechanism<br>FDT measurement |
| 08. – 11.02.2016 | Tokyo (JP) | NFC Forum Members Meeting | IFAT: Wörle / Hölzl / Khemani | Analog Technical Specification<br>Progress in Analog harmonization |
| 07. – 10.03.2016 | Tokyo (JP) | ETSI SCP TEST48 | IFAT: Riegebauer | TS102622 Rel-12, backward/forward compatibility |
| 05. – 06.04.2016 | F2F Gratkorn (AUT) | Digital Working Group (NFC Forum) | IFAT: Wörle | Digital Protocol Specification 2.0 |

| | | | | |
|---|---|---|---|---|
| 20. – 21.04.2016 | F2F London (UK) | TC EMVCo Alignment Taskforce (NFC Forum) and L1WG (EMVCo) | IFAT: Wörle | Harmonization of Analog Parameters NFC Forum<-> EMVCo |
| 17.05.2016 | F2F Munich (DE) | NFC Forum, GSMA, STA and other international Public Transport Experts | IFAT: Wörle | Harmonization of Analog Parameters<br>ISO<->NFC Forum |
| 06. – 09.06.2016 | IFX Graz (A) | ETSI SCP TEST49 | IFAT: Riegebauer | Test spec for the SE tests<br>Lower layer (SWP, CLT) tests |
| 13. – 17.06.2016 | Dallas (U.S.A.) | NFC Forum Members Meeting | IFAT: Wörle / Hölzl<br>IFAG: Schmidt / De Lera | Analog harmonization to ISO/IEC 14443 and EMVCo |
| 27.07.2016 | Conf Call | TC EMVCo Alignment Taskforce (NFC Forum) and L1WG (EMVCo) | IFAT: Wörle | Harmonization of Analog Parameters NFC Forum<-> EMVCo |
| 13. – 15.09.2016 | ETSI Campus Sophia Antipolis (F) | ETSI SCP TEST50 | IFAT: Riegebauer | Focus on Rel-12 (APDU channel...) |

Table 1: International standardisation activities by partner IFAT

## Activities by partner GTO

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| 28. – 30.01.2014 | Kochel (Germany) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | Evaluation of Phase measurements methods |
| 8. – 9.04.2014 | Neuchâtel (Switzerland) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | Tests results on phase measurement methods |
| 23. – 25.09.2014 | Salamanque (Spain) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | |
| 24. – 26.03.2015 | Hiroshima (Japan) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | |
| 23. – 25.09.2015 | Vienna (Austria) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | |
| 2. – 4.02.2016 | Kyoto (Japan) | ISO SC17 WG8 and TF2 | GTO: Jean-Paul CARUANA | |

Table 2: International standardisation activities by partner GTO

## Activities by partner AMS

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| 28 – 30.01.2014 | Kochel am See (Germany) | ISO SC17 WG8 and TF2 | AMS: Maksimilian Stiglic | Analog Technical Specification |
| 23 – 27.02.2015 | HHiroshima City Cultural Exchange Hall<br>Iroshima (Japan) | ISO SC17 WG8 and TF2 | AMS: Maksimilian Stiglic | Analog Technical Specification<br>Phase Drift Analysis in Active PICC and Evaluation of Passive and active cards |

| | | | | |
|---|---|---|---|---|
| 08 – 09.04.2014 | Institute de Microtechnique – Neuchatel (IMT) – Neuchatel (Switzerland) | ISO SC17 WG8 and TF2 | AMS: Maksimilian Stiglic | Extension of PICC and PCD test methods |
| 22 – 23.09.2015 | ASI Austrian Standard Institute | ISO SC17 WG8 and TF2 | AMS: Maksimilian Stiglic; Giuliano Manzi | Phase Drift Analysis in Active PICC and Evaluation of Passive and active cards<br>Extension of PICC and PCD test methods |
| 24 – 28.03.2014 | San Francisco CA (USA) | NFC Forum PLUGFEST | AMS: Bee Peng, Oliver Regenfeld | |
| 01 – 05.06.2015 | Shanghai (China) | NFC Forum | AMS: Oliver Regenfelder | |
| 19 – 23.10.2015 | Vancouver (Canada) | NFC Forum | AMS: Oliver Regenfelder | |
| 05. – 06.04.2016 | Gratkorn (Astria) | NFC Forum | AMS: Oliver Regenfelder | |

Table 3: International standardisation activities by partner AMS

## 2.2 Standardisation for Security and Privacy

In the field of security and privacy based on cryptographic methods the MATTHEW project team was especially active through its scientific leader, Dr. Pascal Paillier, who has a long record in the field and is an accepted expert in the international community. The ISO standardisation sub-committee SC27 “IT Security Techniques” is the roof under which standardisation of cryptographic methods for security and privacy are handled, elaborated and fixed as international standards.

## Activities by partner CRX

The ISO sub-committee 27 (SC 27, Security Techniques) is dedicated to IT security. It is formed of 5 working groups, among which the Working Group 5 (WG5) has a particular focus on Identity Management and Privacy. The entire ISO SC 27 (all 5 Working Groups) meets physically twice a year, with a spring meeting and a fall meeting.

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| 11. – 15.04.2016 | Tampa (USA) | ISO SC27 WG2 and WG5 | CRX: Pascal Paillier | Cryptography and security mechanisms (WG2), and Privacy (WG5) |
| 26. – 30.10.2015 | Jaipur (India) | ISO SC27 WG2 and WG5 | CRX: Pascal Paillier | Cryptography and security mechanisms (WG2), and Privacy (WG5) |
| 4. – 8.05.2015 | Kuching (Malaisia) | ISO SC27 WG2 and WG5 | CRX: Pascal Paillier | Cryptography and security mechanisms (WG2), and Privacy (WG5) |
| 20. – 24.10.2014 | Mexico City (Mexico) | ISO SC27 WG2 and WG5 | CRX: Pascal Paillier | Cryptography and security mechanisms (WG2), and Privacy (WG5) |
| 07. – 11.04.2014 | Hong-Kong (China) | ISO SC27 WG2 and WG5 | CRX: Pascal Paillier | Cryptography and security mechanisms (WG2), and Privacy (WG5) |

Table 4: International standardisation activities by partner CRX

During the run time of the MATTHEW project pre-work for an ISO standard on ABCs has been successfully performed and in the meanwhile this standard has been elaborated towards a working draft. This process had been performed in three phases:

- Phase 1 (spring 2014, fall 2015): the joint study period on ABCs
- Phase 2 (fall 2015, spring 2016): the study period on PPABEA (Privacy-Preserving Attribute-Based Entity Authentication)
- Formulation of a new ISO/IEC standard in Working Draft stage (release in October 2016)

# Chapter 3 Standardisation on national level

Standardisation on national level usually happens in close interaction to the international standardisation. In this interaction the national meetings have two main issues, first to nominate national delegates to the international committees and second to prepare proposals and discuss national alignment on proposals and drafts before discussion on international level. With such national alignments the position of a delegate can be much better elaborated and better standing in the international context can be achieved, especially if contributions from several important industrial players can be already discussed and aligned on the national level.

Since the main industrial partners of the MATTHEW project are located in France and in Austria, this chapter focusses on the national activities of these two countries, although the expertise of Austrian colleagues is also represented in e.g. the relevant German DIN entities.

## 3.1 France

France has always been strong in standardization efforts on national and international level. The various AFNOR groups serve as a national body to align French positions in standardisation processes. In the following table two MATTHEW-relevant activities with respect to national standardisation of active transmission technology are listed:

**Activities by partner GTO**

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| | Paris (France) | AFNOR | GTO: Jean-Paul CARUANA | Analysis and test method presentation |
| 10.09.2014 | Paris (France) | AFNOR | GTO: Jean-Paul CARUANA | National alignment |

Table 5: MATTHEW relevant standardisation activities in France

## 3.2 Austria

In Austria the Austrian Standards Institute https://committees.austrian-standards.at/ act as the national pendant for the international standardisation entities, for example ASI K220 is the national mirror of CEN TC278 und ISO TC204 and ASI K001.AG17 is the national mirror of ISO/IEC JTC1 SC17.

**Activities by partner IFAT**

| Date | Place | Working Group | Representatives | Topics |
|---|---|---|---|---|
| 11.12.2015 | Vienna | ASI K220 | IFAT: Riegebauer | ISO TC204 NWI Technical guidelines for Interoperability |
| 31.03.2016 | Klagenfurt | ASI K001 | IFAT: Riegebauer / Gruber | ECMA fast-track ballot for 2 NFC-SEC standards approved |
| 13.05.2016 | Vienna | ASI K220 | IFAT: Riegebauer | prCEN TS 16794-1/-2 “Public transport — Communication between contactless readers and fare media” APPROVED w/o comments |
| 23.09.2016 | Vienna | ASI K001 | IFAT: Riegebauer / Gruber | B. Zwattendorfer (IFAT) approved as Austrian Delegate to SC17 WG3, WG10, WG11 |

Table 6: MATTHEW relevant standardisation activities in Austria

# Chapter 4 Conclusions

As can be seen from their strong engagement in the standardisation processes MATTHEW project partners are aware of the positive impact of standardisation on the mass product markets. Especially the harmonisation between different standardisation groups like ISO, NFC-Forum and EMVCo has become a very prominent topic, since a multi-discipline approach has to be followed to achieve interoperability. All parties have their special focus, may it be physical layer of data transmission, integration in devices, like smart phones and tablets or the application level concerning banking, access control or public transport schemes. Only if the interfaces between the various viewpoints are also considered, seamless integration and positive end user experience can be achieved.

Thus this report highlights the successful participation of MATTHEW project members in international standardisation committees based on detailed work performed inside their individual partner institutions, in the MATTHEW project team, and on the level of national standardisation bodies.

# Chapter 5 List of Abbreviations

| | |
|---|---|
| AFNOR | Association française de normalisation |
| ASI | Austrian Standards Institute |
| CEN | Comité Européen de Normalisation |
| DIN | Deutsches Institut für Normung |
| EMV | Europay, MasterCard, and Visa |
| EMVCo | EMV Corporation |
| ETSI | European Telecommunications Standards Institute |
| HCI | Host Controller Interface |
| ISO | International Organization for Standardization |
| JTC | Joint Technical Committee |
| NFC | Near Field Communication |
| PCD | Proximity Coupling Device |
| PICC | Proximity Integrated Circuit Card |
| SC | (Standardisation) Sub-Committee |
| SCP | Smart Card Platform |
| SWP | Single Wire Protocol |
| TC | Technical Committee |
| WG | Working Group |