matthew

D7.2

Updated Plan and initial report on Dissemination and Exploitation

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 (R)
Deliverable reference number:	ICT-610436 / D7.2 / Final | 1.0
Activity and Work package contributing to the deliverable:	WP 7
Due date:	June 2015 – M20
Actual submission date:	26.06.2015

Responsible organisation:	IAIK
Editor:	Erich Wenger
Dissemination level:	Public
Revision:	1.0

Abstract:	This report details the dissemination and exploitation activities, which have been ongoing during the first halve of the MATTHEW project, mainly focused on increasing its visibility and the public awareness of the project on starting to disseminate technical results. For instance, several technical papers have already been published. The standardisation & exploitation prospects are still in line with those defined in the DoW.
Keywords:	Dissemination, Standardisation, Exploitation, IPR

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

Erich Wenger (IAIK)

Contributors (ordered according to beneficiary numbers)

Holger Bock (IFAT)

Christian Dietrich (GTO)

Martin Deutschmann (TEC)

Christian Hanser (IAIK)

Sandra Moschitz (TEC)

Jiri Havlik (IMA)

Disclaimer

Executive Summary

This deliverable reports on the progress of the project partners in terms of dissemination of the project and exploitation of project results during the first and a half years of the MATTHEW project.

To further raise the public level of awareness of the project within the scientific and industrial communities, a diversity of dissemination activities have been impelled, including a project website as well as presentations at workshops and conferences.

The consortium analyzed in detail the mobile access control market to find out about exploitation opportunities of the project, defined individual plans and generated ideas for future MATTHEW implementations.

The following falls under the achievements and work towards the project goals of the first 20 months of the MATTHEW project for dissemination:

- 10 peer-reviewed scientific publications
- 11 events (workshops, conferences etc.) were used to present the MATTHEW project, its work status and objectives
- 8 further publications disseminated the project to international audience
- a project website, links on partner websites, a project logo and leaflet underpin the professional dissemination management within the MATTHEW project

Contents

List of Figures

List of Tables

Chapter 1 Introduction

The goal of the MATTHEW project is to enable new applications and services on mobile platforms based on “multiple roots of trust” with distinct characteristics, to develop novel methods overcoming the limitation of today’s passive NFC transmission technologies by active modulation, and to show new ways of exchanging the roles from one mobile platform to another. With various technology readiness levels, these goals are directly related to the on-going dissemination and exploitation activities.

In this document the MATTHEW consortium documents the efforts and intentions to promote the project amongst stakeholders, engage the target audience and maximize the uptake of project results.

This document is mainly split in two parts. Chapter 2 discusses MATTHEW efforts to disseminate our results within the scientific community, the industry, the civil society, policy makers, and others. It discusses stakeholders as well as MATTHEW’s public appearances, its scientific publications, and its social media strategies. Chapter 3 documents MATTHEW’s exploitation plans. Therefore we address the current market as well as state the current, updated exploitation plans of all partners.

Chapter 2 Dissemination

Dissemination activities ensure the visibility and awareness of the project and support the widest adoption of its results in industry and research. The strategy for the dissemination of MATTHEW aims at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties. This chapter analyzes the different stakeholders and how they are addressed, lists the dissemination activities performed by the project partners and underpins the impact of the public website.

2.1 Stakeholder Analysis

Within the MATTHEW project, special attention is paid to target-oriented dissemination activities in order to address stakeholders properly. All dissemination activities will contribute to the overarching objectives of creating awareness, increasing involvement, understanding and promotion of the project outcomes among the following clearly defined target groups:

- Scientific Community and higher education
- Industry
- Civil Society
- Policy Makers
- Medias
- Others

The dissemination objectives differ depending on the defined target groups, whereas each target group receives individual messages via specific communication channels like website, press, events etc. Key messages will emphasize both, the scientific as well as the business perspective. The following matrix gives an overview about why and how the defined stakeholders will be addressed.

Stakeholders	Targeted addressing of dissemination stakeholders		
	WHO	**WHY**	**HOW**
Scientific community and higher education	universities, research institutes, experts, scientific publication bodies	Inform the research community about developments and their impact. Engage co-operations.	Scientific Publications, project presentation, participation in conferences, workshops; project liason meetings (with e.g. HINT)
Industry	partners, global players, up- and downstream supply chain industries	Emphasize technological advantage, promote to appliers and receive feedback	Partner promotion, contributions to events, presentations, networking sessions
Civil Society	opinion leaders, Chief Security Officers (CSO) of companies and institutions	Include civil society representatives into security debates and present project outcomes and advantages	Press Releases, Project News on partner websites, project website, presentations at fairs and events

Stakeholders	Targeted addressing of dissemination stakeholders		
	WHO	**WHY**	**HOW**
Policy Makers	national and international public organizations as well as European institutions, programme committees	Create awareness with regards to the political relevance of security topics and their societal impact.	Contribution to EC yearbook 2014, participation in events (CSP Forum)
Medias	newspapers, TV, press, innovation forums, etc.	Raise project awareness for a wide target group through presence in press and (social) media	Press Releases, Interviews, Website, Social Media (Twitter)
Others	e.g. end users, partner company internals	Promote the critical innovations of the project in order to accelerate market adoption	Relation to other projects, news, partner promotion

Table 1: Dissemination Stakeholders

According to the matrix established above, stakeholders will be identified and addressed during the MATTHEW project lifecycle. The lists in section **Error! Reference source not found.** provide an overview of the dissemination activities within the project and which target group has been addressed.

2.2 Visual Identity of the project

The creation of a corporate visual identity plays a significant role in the way the MATTHEW project presents itself to both internal and external stakeholders. A corporate visual identity expresses the values and ambitions of our project and its characteristics. Our corporate visual identity provides the project with visibility and "recognizability". It is of vital importance that people know that the organization exists and remember its name and core business at the right time. The following subchapters present the actions, which were taken in order to create a visual identity of the project.

2.2.1 Logo

For the improvement of its visibility, the MATTHEW project has adopted a project logo. The logo is used on all internal templates as well as on external dissemination tools.

Figure 1: Project logo

2.2.2 Leaflet

The official MATTHEW leaflet is a four page informative and graphically appealing A4 flyer, highlighting the objectives and the work programme of MATTHEW. It can be, and has already been used for distribution at conferences or certain other events in order to provide further visibility to the MATTHEW project. TEC was mainly responsible for the content and design of the leaflet and distributed it to all partners after finalisation. An electronic version of

the leaflet is available on the MATTHEW website, following: http://matthew-project.eu/downloads/MATTHEW_Leaflet.pdf

Figure 2: MATTHEW leaflet

2.2.3 Project website

For greater visibility of the project, a website was launched in month 2. It provides an overview of the project and up-to-date information on its activities and results, as well as contact details, partner information and information on events. The website is based on the Content Management System (CMS) "Joomla!", a webserver which provides the public website of the project and additionally restricted areas for members only. The website can be viewed with a standard web browser and will be kept alive throughout the project period and at least 3 years afterwards. The project website has been designed to be easily accessible and give an introduction to the project.

The MATTHEW project website is available at the following link: http://www.matthew-project.eu

Figure 3: Screenshot of the MATTHEW homepage

The project website serves as the most versatile information and communication tool, because on the one hand it provides the opportunity to provide information for a worldwide audience and on the other hand enables a working platform for the project team.

Besides the public area, there is a password-protected area, reserved for project participants, in order to share project-internal data only. Only registered partners are able to enter it and can benefit from the options offered there. These include for example:

- Calendar for appointments and meetings,
- Mailing lists for reaching special mailing groups,
- Archives of the mailing list emails.

The overall goal of the MATTHEW website is to enhance the level of awareness. Shortly tools were established in order to be able to measure various indicators (number of visitors,

pages etc) over the project lifetime. Therefore, two major tools have been established, which verifies the data generated by the other tool.

2.2.3.1 Website Updates

The MATTHEW website was further enhanced and partially re-designed, to include more dynamic features and to thereby transform it into a more proactive platform for dissemination activities (as suggested in Recommendation 4 of the first annual review).

For this purpose additional Joomla tools and modules were installed, which allow to highlight the most recent news, upcoming meetings/conferences and actual publications/deliverables.

Furthermore a blog tool was installed, which can be used for relevant postings such as reached milestones or any other news. The blog tool will be used as an interactive platform for communicating and publishing information to the external audience, as soon as the enabling at IFAT communication department has been taking place.

Further a toolbox is made available with downloadable (open source) software/libraries provided by partners, such as an Elliptic Curve Cryptographic (ECC) Library in C or an ECC breaker, provided by partner TU Graz: http://www.matthew-project.eu/news

2.2.3.2 Website analysis

A statistical analysis of access (both unique visitors and overall visits) to the MATTHEW project website for a graphical visualization has been created which can be found below. In order to obtain these figures, we used two different statistical tools. The following figures give attention to the period from 1st of June 2014 to end of June 2015.

The two illustrations below provide an overview of the number of unique visitors and the total number of requests (visits). While the visitors are counted just for the first time of their website visit, visits are counted for each request of the website.

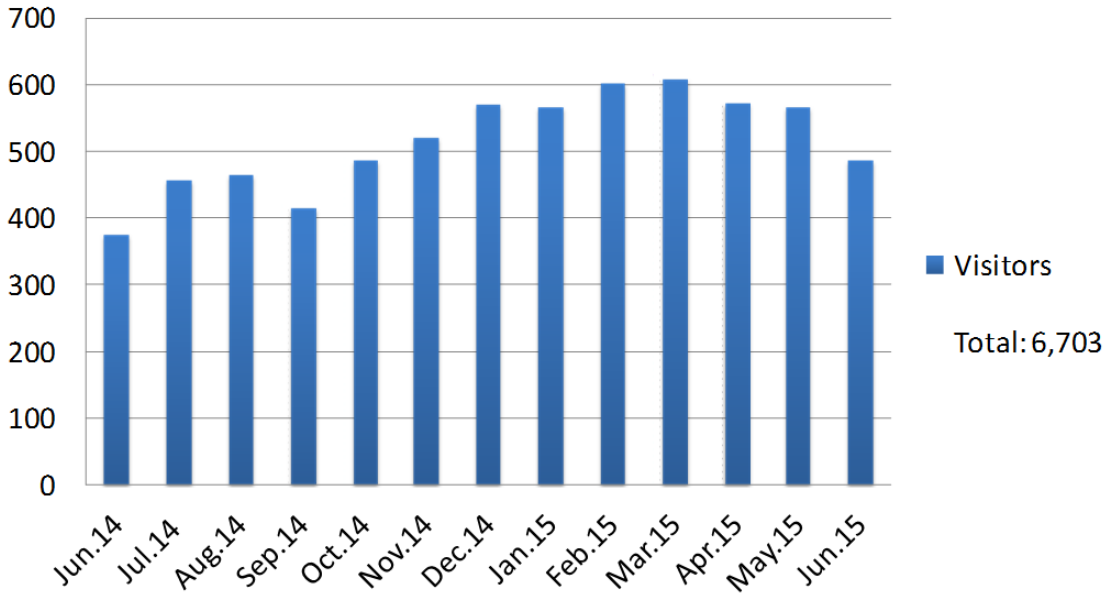


Figure 4: MATTHEW website statistic of unique visitors (June 2014 – June 2015)

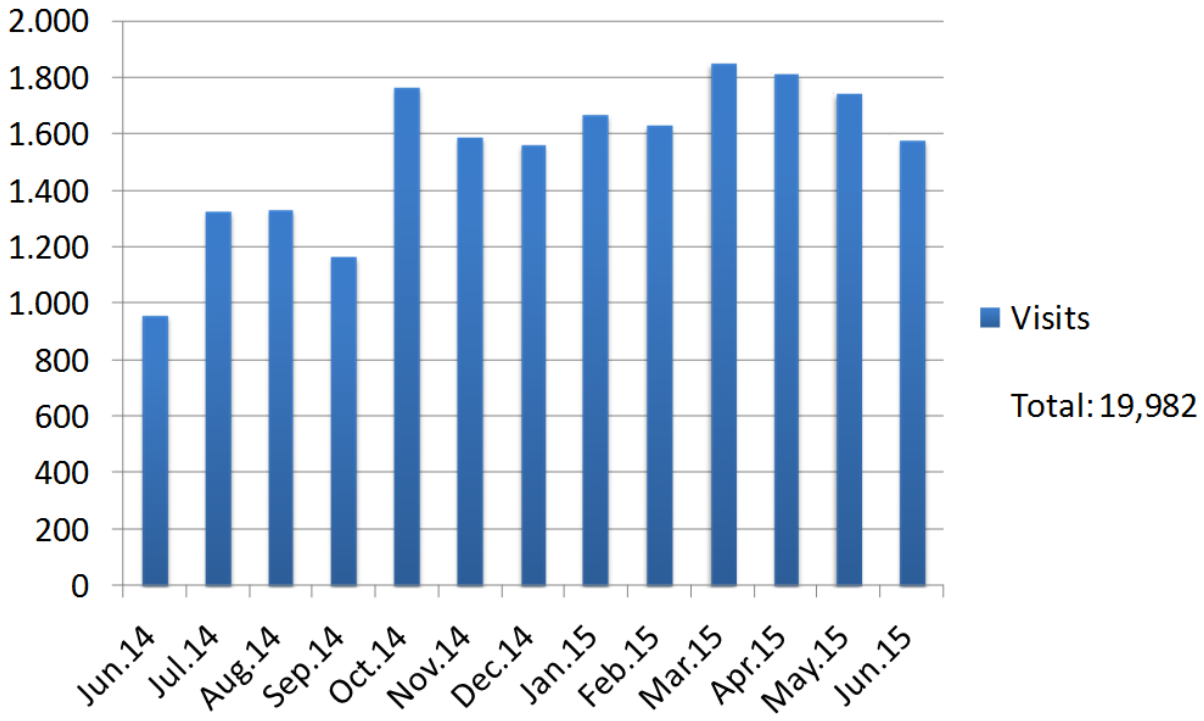


Figure 5: MATTHEW website statistic of non-unique visits (June 2014 – June 2015)

During the last 13 months the MATTHEW website has been visited 18,405 times in total by 6,215 unique visitors. As obvious in the two figures before, there is a steadily increase of visits (as well as visitors) visible during the last year.

2.3 Dissemination Activities

The project and its results have been disseminated by invited talks at conferences, by publications at scientific and industry oriented conferences and by organising technical workshops within the project. The following section presents our dissemination activities in order to document the extent to which we have executed our above mentioned dissemination strategy.

2.3.1 Scientific Publications

The following scientific peer-reviewed publications have been published within the first 20 months of the MATTHEW project. All scientific publications are listed in an action overview list and are updated by the partners on a regularly base. Currently 10 peer-reviewed scientific publications were prepared during the first 20 project months.

Title	Main authors	Title of the periodical or the series	Publisher	Year of publication	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster	Erich Wenger	Selected Areas in Cryptography - SAC 2014	Springer International Publishing	2014	Doi:10.1007/978-3-319-13051-4_22	yes
Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices	Thomas Unterluggauer	Ninth International Conference on Availability, Reliability and Security (ARES) 2014	IEEE Computer Society	2014	doi:10.1109/ARES.2014.16	yes
Efficient Pairings and ECC for Embedded Systems	Thomas Unterluggauer	Cryptographic Hardware and Embedded Systems - CHES 2014	Springer Berlin Heidelberg	2014	doi:10.1007/978-3-662-44709-3_17	yes

[1] A permanent identifier should be a persistent link to the published version full text if open access or abstract if article is pay per view or to the final manuscript accepted for publication (link to article in repository).

[2] Open Access is defined as free of charge access for anyone via Internet. Please answer "yes" if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.

Title	Main authors	Title of the periodical or the series	Publisher	Year of publication	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms	Thomas Korak	Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2014	IEEE Computer Society	2014	doi:10.1109/FDTC.2014.11	yes
Clock Glitch Attacks in the Presence of Heating	Thomas Korak	Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2014	IEEE Computer Society	2014	doi:10.1109/FDTC.2014.20	yes
Location-dependent EM Leakage of the ATxmega Microcontroller	Thomas Korak	Foundations and Practice of Security	Springer International Publishing	2014	doi:10.1007/978-3-319-17040-4_2	yes
Harder, Better, Faster, Stronger - Elliptic Curve Discrete Logarithm Computations on FPGAs	Erich Wenger	Cryptology ePrint Archive	IACR	2015	http://eprint.iacr.org/2015/143	yes
Suit up! Made-to-Measure Hardware Implementations of Ascon	Hannes Groß	Digital System Design (DSD), 2015 18th Euromicro Conference on	IEEE Computer Society	2015	http://eprint.iacr.org/2015/034	yes
Practical Round-Optimal Blind Signatures in the Standard Model	Christian Hanser	CRYPTO 2015	Springer Berlin Heidelberg	2015		yes
Verifiably Encrypted Signatures: Security Revisited and a New Construction	Christian Hanser	ESORICS 2015	Springer Berlin Heidelberg	2015		yes

Table 2: List of scientific publications

2.3.2 Further Publications, Workshops, Presentations

All Presentations, Conferences and Workshops are listed in an action overview list and are updated by the partners on a regularly base. Currently the MATTHEW partners participated in 21 presentations, conferences and workshops during the first 20 project months.

Type of activity	Main Leader	Title	Date	Place	Type of Audience	Size of audience	Type and goal of the event	Countries addressed
Workshop	IMA	Workshop for VIP customers	5.12.2013	Prague, Na Valentince 1003/1	industry	30	Important customers informed about new technology of IMA.	National
Web	IMA	Company web site	2013	Online	scientific society, industry, civil society, policy maker, media, other	/	Overall company info	International
Other	TEC / All partner	MATTHEW Homepage / Logo	2014	Online	scientific society, industry, civil society, policy maker, media, other	/	http://www.matthew-project.eu / Logo will be used for MATTHEW publications	International
Workshop	IMA	Info Day IMA Praha	4.4.2014	Prague, Na Valentince 1003/1	industry	20	Overall company info	National
Workshop	IMA	Workshop at Technical university in Liberec	16.4.2014	Liberec, TUL	scientific society	40	Overall company info	National
Conference	IMA	Microelectronics in CZ	22.11.2013	Prague, Czech technical university	industry, other	10	Overall company info	National
Workshop	GTO, AMS	ISO14443, Task Force 2 and Working Group 8 Meeting	7.4.2014	NeufChatel , Switherland	industry	25	International standardization	International

Type of activity	Main Leader	Title	Date	Place	Type of Audience	Size of audience	Type and goal of the event	Countries addressed
Publication	IAIK	Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster	15.8.2014	Montreal, Canada	scientific society, industry	/	Dissemination of research results	International
Publication	IAIK	Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices	8.9.2014	Fribourg, Switzerland	scientific society, industry	/	Dissemination of research results	International
Workshop	GTO, AMS	ISO14443, Working Group 8 Preparation Meeting	10.9.2014	Paris, France	industry	15	National standardization	National
Workshop	GTO, AMS	ISO14443, Task Force 2 and Working Group 8 Meeting	22.9.2014	Salamanque, Spain	industry	20	International standardization	International
Publication	IAIK	Efficient Pairings and ECC for Embedded Systems	23.9.2014	Busan, Korea	scientific society, industry	/	Dissemination of research results	International
Publication	IAIK	On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms	23.9.2014	Busan, Korea	scientific society, industry	/	Dissemination of research results	International
Publication	IAIK	Clock Glitch Attacks in the Presence of Heating	23.9.2014	Busan, Korea	scientific society, industry	/	Dissemination of research results	International
Workshop	IMA	Meeting of departments of the Czech Technical Universities	9.10.2014	Kladno, CZ	industry	30	Dissemination of research results	National

Type of activity	Main Leader	Title	Date	Place	Type of Audience	Size of audience	Type and goal of the event	Countries addressed
Publication	IAIK	Location-dependent EM Leakage of the ATxmega Microcontroller	3.11.2014	Montreal, Canada	scientific society, industry	/	Dissemination of research results	International
Conference	IFAT	8th RFID Symposium	4.12.2014	Dresden, Germany	scientific society, industry, civil society, other	45	Dissemination of project results	International
Workshop	IFAT/TEC	Liaison Meeting with HINT project	22.4.2015	Graz, Austria	scientific society, industry, policy maker, other	15	Dissemination of project results	International
Web	AMS	How new 'boostedNFC' technology enables mobile phones and wearable devices to emulate contactless cards reliably	24.4.2015	Graz, Austria	scientific society, industry, civil society, other	/	Dissemination of research results	International
Forum	TEC	DG Connect and CSP Innovation Forum - Digital Security: Cybersecurity, Privacy & Trust	28-29.4.2015	Brussels, Belgium	scientific society, civil society, other	/	Presentation of the MATTHEW project through leaflets and conversations	International
Publication	IAIK	Practical Round-Optimal Blind Signatures in the Standard Model	16.8.2015	Santa Barbara, USA	scientific society, industry	200	Dissemination of research results	International

Table 3: List of dissemination activities

2.3.3 Other dissemination Activities

- **Project Announcement Letter**

The intention of the MATTHEW Announcement Letter was to communicate the project start and ideas towards the general public. It was released in January 2014 giving a summary of the project addressed to non-specialist citizens and outlines what the project is about and how its planned results would matter for citizens and consumers. It can be found on the MATTHEW website following:
http://matthew-project.eu/downloads/MATTHEW_AnnouncementLetter.pdf

- **Interview for EU Yearbook**

Based on an interview given by the Coordinator, an article about the MATTHEW project will be published in the EU Yearbook.

2.3.4 Social Media Strategy

After fixing the internal processes within Infineon as the project leader, it was decided to create a dedicated *Twitter* account for the MATTHEW project. A communication strategy was decided in the consortium and going live was scheduled for July 15th, 2015.

Chapter 3 Exploitation

Exploitation is recognised as the key enabler for the success of the MATTHEW project. Hence, all MATTHEW partners are aware of and committed to the exploitation of the project results. It is the principle of all exploitation activities to use research results to create value within all participating organisations and thus to improve their competitive advantage. Only by scaling up the results into commercial offerings, all European constituents can be reached while ensuring profitability through economies of scale. This chapter analyzes the market and its developments and describes the exploitation plans of the MATTHEW partners.

3.1 MATTHEW addressed market overview

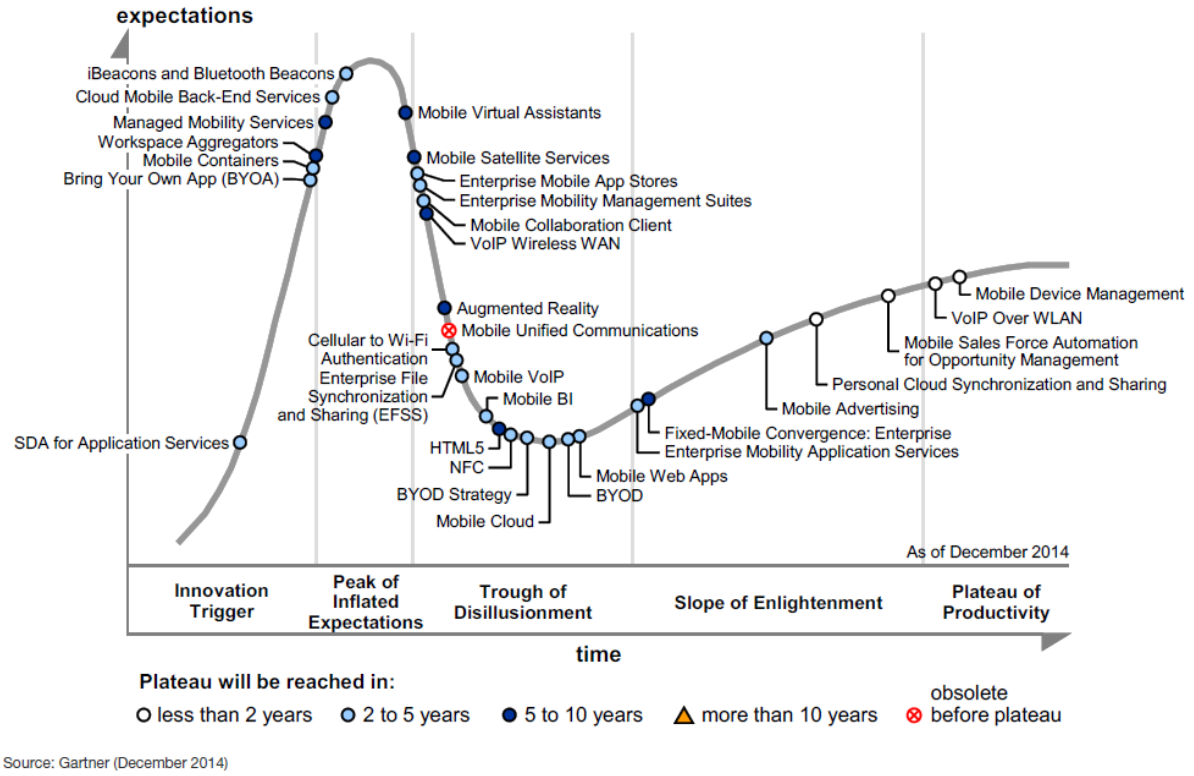
This section intends to describe the main market evolution that may affect the exploitation and dissemination plan targeted by the MATTHEW project partners. The initial concept and objective in the MATTHEW Description of Work has been confirm to be true and even evolving further confirming the need for the "Multiple Root of Trust" allowing the transferability of credentials between these devices and compliancy with the privacy regulations under definition.

As foreseen the number of security relevant devices in ICT systems for mobiles services extending since 2013 with the development of the Internet of Things market and the introduction of several wearable objects: bracelets, jewels, watches… most of the time these devices often put the mobile platform at the heart of the user security component network.

The mobile devices are continuously integrating new technologies to improve the ease of use and extend the suite of connected equipment all this to enlarge the services available to the end user in mobility. These evolutions have to be considered in the definition of the MATTHEW platform to ensure for its adaptation and ensure deployment plan foreseen by the partners.

As identified in the studies from Gartner: the Hype Cycle for Mobile Device Technologies (July 2014) and the Hype cycle for mobile software and services (December 2014), the integrated communication technologies have strongly been improved:

- For network and internet connectivity, with the convergence between mobile, satellite and fix network services (improvement of the cellular to WiFi authentication), the introduction of LTE in conjunction and the deployment of mobile cloud base services by operators and device manufacturer, … Associating these evolution with the multiplication of user owned devices (tablets, laptops, mobiles, watches…), the mobile platform is becoming more a "viewing terminal" than a storage device, thus the user request for local memory extension is drastically reducing to the favour of network centralised data. This trend enforced by the deployment of Enterprise based services and the BYOD approach. The device manufacturer use this opportunity to address their design constraints by removing the microSD interface, as already done by Apple in the iPhone for years and recently by Samsung in the S6 device.



Source: Gartner (December 2014)

Figure 6: Hype Cycle for Mobile Software and Services

- For proximity communication, the NFC and Bluetooth are the key support technologies for establishing to equipment surrounding the user environment such as terminals for transactions or wearable devices (earpiece, watch, keyfob…) to setup the user network of devices.

The Bluetooth technology with proximity detection (beacon) and the raising support of the Bluetooth Low Energy (BLE) is currently driving the implementation of simplified mobile payment, access control, information delivery and monitoring/positioning services, as adds additional and seamless (without cables) communication streams to the context in which the end user evolves.

The NFC technology is now in all major smartphone OS vendors as in addition to Android (Acer, Asus, HTC, Huawei, Lenovo, LG, Motorola, Samsung, Sony and ZTE), Blackberry, Windows Phone (Nokia and Samsung), even Apple joined the movement in September to include it in the iPhone 6 with the launch of the Apple Pay payment solution. With this integration the hardware and software companies hope to move beyond payments, for which NFC was initially targeted, and provide the developer community with another tool to foster innovative applications as we will see in the contactless market evolution. As a result the deployment of NFC handset is growing faster than initially planned in the DoW and described in the figures below by end of 2015 more than 1 billion NFC handset will be deployed.

Table 1: Installed Base of Mobile Subscribers and NFC Handsets
World Market, Forecast: 2013 to 2019 *(Source: ABI Research)*

Installed Base	Units	2013	2014	2015	2016	2017	2018	2019	DIFF 14-19	CAGR 14-19
Mobile Subscribers	(Millions)	7,026.66	7,429.05	7,767.47	8,050.76	8,258.32	8,433.29	8,584.74	1,155.69	2.90%
NFC Handsets	(Millions)	347.98	639.28	1,090.09	1,675.96	2,259.54	2,850.31	3,450.54	2,811.26	40.10%
NFC Penetration	(%)	5.00%	8.60%	14.00%	20.80%	27.40%	33.80%	40.20%	-	36.10%
YoY Growth for NFC Installed Base	(%)		83.70%	70.50%	53.70%	34.80%	26.10%	21.10%	-	-

Figure 7: Installed Base of Mobile Subscribers and NFC Handsets

In addition to the important deployment of NFC mobile, in the last 2 years the role of the TSM (Trusted Service Manger) has been established to manage proximity based services / transactions using NFC and a secure element, initially targeted for the mobile payment market it can address eTicketing, transportation, access control retail, loyality. This role is to support the setup of different business model and the deployment of the NFC services independently of the location and ownership/issuer of the secure element. The deployment of the requested architecture, and the difficulty for setting up business models satisfying the different actors, lead non MNOs service providers to look for alternative local connectivity solutions (e.g. Bluetooth) or alternative NFC solution bridging or add-on solutions, non SIM based such as eSE making use of the eSE integrated by the OEM in the mobile, µSD NFC or HCE (Host Card emulation) platform with the OTT (Over The Top) players or financial institutions. The projection below from ABI research on the NFC bridging solution clearly highlight the fact that these NFC alternatives are reaching market saturation, apart for the µSD which did not consider the impact of other alternatives deployment such as wearables and HCE by Financial Institutions.

Table 155
NFC Bridging Solution Shipments, ASPs, and Revenues by Type
World Market, Forecast: 2011 to 2019

(Source: ABI research)

Bridging Solution Type	2013	2014	2015	2016	2017	2018	2019	CAGR 14-19	SUMM 14-19
Foils/Flex	5 718 257	6 435 269	6 974 181	7 605 819	7 028 786	6 117 454	5 075 810	-4,6%	39 237 318,20
Micro SD	3 638 712	4 709 838	6 229 841	7 910 606	8 948 097	10 008 432	11 109 375	18,7%	48 916 188,65
Connected Sticker & Sleeves	558 524	1 524 697	2 114 251	1 976 510	1 211 981	984 725	1 015 282	-7,8%	8 827 446,74
Contactless Unconnected Stickers	17 049 016	26 946 967	25 088 098	26 599 744	25 218 685	25 933 194	28 862 660	1,4%	158 649 347,91
Total	26 964 509	39 616 771	40 406 372	44 092 679	42 407 549	43 043 805	46 063 127	3,1%	255 630 301,50

Figure 8: NFC Bridging Solution Shipments

Indeed one of the global trends identified for the Contactless technology is its integration in several devices such as Wearables for payment, ticketing and access control. As for the Mobile commerce smart wearable devices (SmartWatches), will improve user experience over the complete service life cycle, from purchasing to usage, several pilots have been performed that confirm the high rate of adoption by the end user (e.g. Barclay bPay wrist bands, hand gloves…) depending on the user interface several technical challenges still need to be addressed (eg. Battery life time, displays, size).

The Near Field Communications report from HIS (May 2015) clearly highlights, in the tables and figures below, the impact of this trend on the NFC secure element shipment by device type and the implementation of NFC secure elements into cellular handsets. It appears clearly that the handset and more precisely smartphones are by far the most popular NFC device, other NFC devices (portable computing, stickers or Tag) are forecasted to represent almost 10% by 2018.

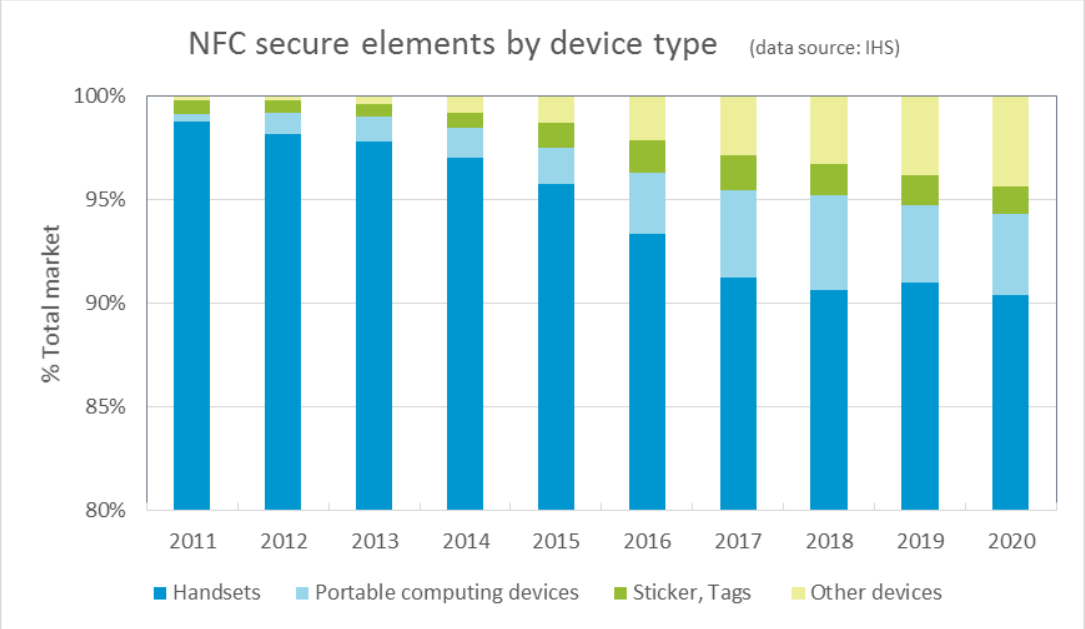


Figure 9: NFC secure elements by device type

The *NFC secure elements embedded into the device* is forecasted to be the most popular implementation (58%) by 2020, followed by the *SIM card* based solution driven by the Mobile Network Operator (22%). The *Other* type of NFC secure element such as NFC stickers and microSD cards, even if they provide more control of the NFC eco system to their issuers (i.e banks), they will represent after having reached its highest share in 2017 (5,6%), the smallest share with 4% in 2020. A new solution appeared in 2013, the *NFC modem combination IC*, that combines the secure element and an NFC front end, is targeted to represent 15,7% market share in 2020 and is the biggest growing segment from 2014 to 2020.This clearly highlights the increasing diversity in the type of NFC secure element implementation.

Table 11 - NFC secure element implementations into cellular handsets
Millions of units shipped 2011 to 2020

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	CAGR 14-20
SIM card	19,8	47,0	76,7	126,5	176,3	220,2	261,8	329,0	394,0	485,6	25,1%
% of Total	41,5%	32,2%	25,4%	31,4%	28,1%	23,2%	21,5%	21,2%	20,8%	22,1%	
Embedded into device	27,7	96,4	214,0	253,0	393,9	594,8	742,0	932,0	1119,5	1275,3	30,9%
% of Total	58,0%	66,0%	71,0%	62,9%	62,8%	62,8%	61,0%	60,0%	59,0%	58,0%	
NFC modem combination IC	0,0	0,0	4,4	12,1	33,3	81,0	144,4	210,1	289,1	345,6	74,8%
% of Total	0,0%	0,0%	1,5%	3,0%	5,3%	8,6%	11,9%	13,5%	15,2%	15,7%	
Other (e.g. SD card)	0,2	2,6	6,3	10,8	23,8	51,1	68,1	82,3	94,9	92,3	42,9%
% of Total	0,5%	1,8%	2,1%	2,7%	3,8%	5,4%	5,6%	5,3%	5,0%	4,2%	
Total secure elements	**47,8**	**146,1**	**301,4**	**402,4**	**627,2**	**947,1**	**1216,4**	**1553,4**	**1897,5**	**2198,8**	**32,7%**
Growth Rate		205,7%	106,3%	33,5%	55,9%	51,0%	28,4%	27,7%	22,1%	15,9%	

Notes: China's SIM pass shipments are included in the SIM card shipment data. In this solution the secure element is embedded in their SIM card.

Source: IHS

Figure 10: NFC secure element implementations into cellular handsets

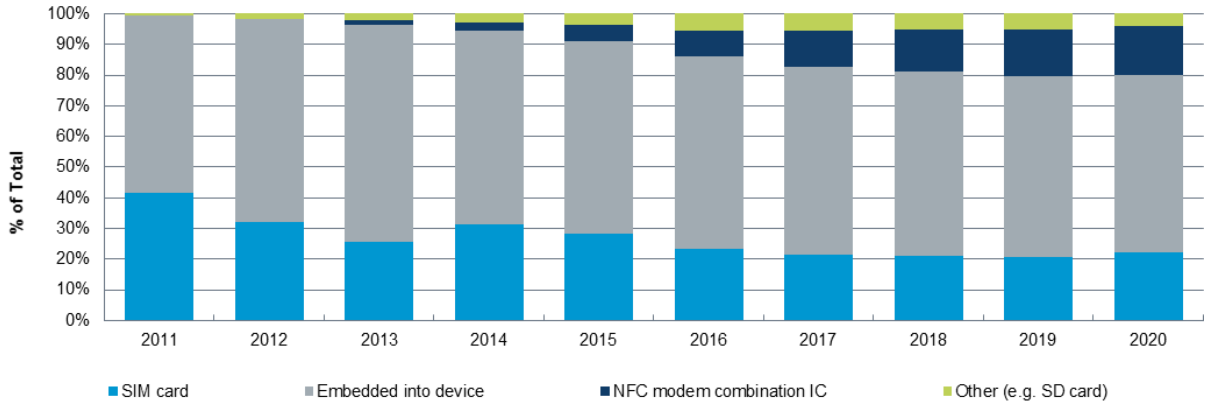


Figure 11: NFC secure element implementations into cellular handsets

The element that disrupted the Contactless market lately and more precisely the payment market is the development of the Tokensisation technologies by OTT, Payments Scheme and finally device makers with the target to remove some of the NFC market lockers. This has been initiated in October 2013, with Google announcement of the support for Host Card Emulation (HCE) on their new Android KitKat operating system, allowing a mobile application on a NFC mobile to emulate in software a smart card, with the support of a network. Which was followed by several announcements from the financial institutions: in February 2014 VISA announced Visa Cloud-Based Payments Program (VCBP) specifications; in March 2014 EMVCo announced the Technical framework for Payment Tokenization and in August 2014, Mastercard publishes MasterCard Cloud Based Payment (MCBP) and the MasterCard Digital Enablement Service (MDES) specifications. This lead the device manufacturer such as Apple to announce in September 2014, Apple Pay which leverages on embedded Secure Element (eSE) and Tokenization technologies; and in march 2015 the announcement from Samsung of the Samsung Pay and by Google of the Android Pay.

The tokenisation technologies have stimulated the NFC market and the adoption of the NFC technology, by adapting to the existing infrastructure thus simplifying the deployment of NFC infrastructure. As these solutions request large and constant network connectivity and are based on the level of security of the mobile device, exposed to malware and security attacks, these payment solution will coexist with Secure Element based solution, and even support their deployment.

One of the key blocking points for NFC based solution was the deployment of the NFC infrastructure. This has been clearly happening with the deployment in the US of NFC compatible POS for the EMV Migration that is ongoing. The 2 major POS manufacturer indicated that the overwhelming majority of terminals now shipped are NFC enabled. As depicted in the figure below the deployment has started in the UK at the end of 2011 with an important raise since of the deployed NFC terminal.

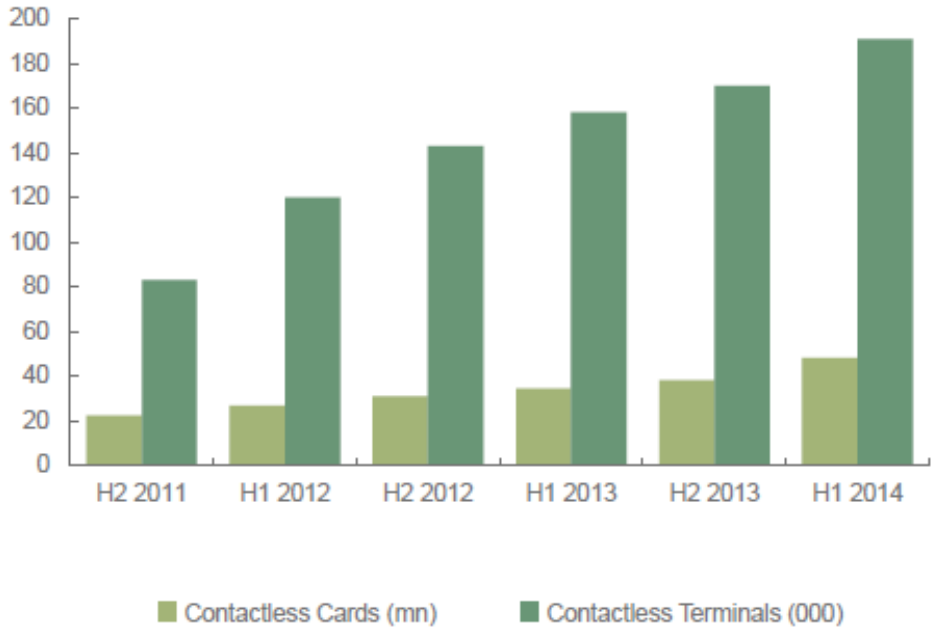


Figure 12: UK Contactless Market

Mobile Ticketing MARKET

As outlined in the Juniper research, MOBILE & ONLINE TICKETING market trends, from March 2015, the Digital ticketing is evolving rapidly adapting to the technologies available to simplify user. The study shows an important move from online to mobile ticketing. The chart below clearly outlines the growth that happened from 2013 to 2014 of mobile tickets purchased via mobile devices across the different sectors: Entertainment Events, Sport events, Airline, Metro/Bus, Rail Tickets.

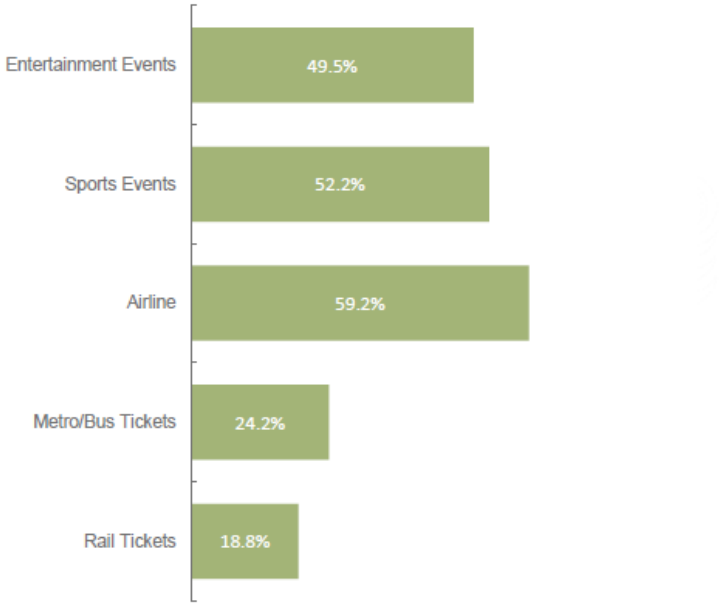


Figure 13: Tickets Purchased via Mobile

This overall provides a great opportunity for the deployment of NFC based solution but here NFC technology is competing with alternative solutions such as SMS or QR codes. The use of the mobile phone for the full mobile ticket lifecycle is the ultimate aim of mobile ticketing and the goal of most operators and ticketing organisations. Fully Integrated Mobile Services: Mobile booking, purchase, payment and delivery can be done using any technology (from SMS to app) and also includes NFC. The study also confirms a strong push towards a fully integrated mobile device that will include wearable device ticketing. This Mobile integration allows providing end user services appropriate to the context (location, time, traffic…) and requests (destination, maps…). This trend is further stimulated by deployment of fully integrated solution such as Apple Pay service integrated in the Apple Passbook wallet.

Mark Dewell from Advanced Ticketing clearly mentioned the practical issue of ticket transferability that addressed in the 3rd use case of MATTHEW project. Many mobile ticketing solutions are based on the assumption that the purchaser of the ticket is also the same person that will board the train or attend the event. This is not necessarily true and the limitations of such assumptions are particularly noticeable in sports ticketing, where one family (or group) member may buy the (physical) tickets and then hand them out prior to entering the sports arena.

3.1.1 Mobile Access Control MARKET

Besides products from other partners, there are several mobile access control systems that have been developed and are distributed by IMA:

3.1.1.1 NFCporter and PATRON-PRO (both IMA portfolio)

The NFCporter system is designed for maximum compatibility with current access control systems of IMA as well as the most frequent identification cards standards. It is therefore prepared for installation at places where most people still use contactless cards and ensures the parallel functioning of both technologies for an unlimited period of time. From the viewpoint of any access control, an attendance or other superior system the identification via mobile phone is identical to the identification using a contactless card. All one has to do is to replace the readers and the NFCporter takes care of the rest. The user identification is as easy as tapping the NFCporter reader with a mobile phone. The user ID is transferred within a second. The ID is then passed on to a superior identification system in order to validate the user rights and unlock the entrance. All communication is carried out at the same speed as when using a contactless card.

PATRON-PRO is an innovative access control system controlled from a mobile phone. The PATRON-PRO mobile app is used for complete access rights administration, simple attendance monitoring and advanced behaviour settings of the system. The system features are:

- Complete administration from a mobile phone
- Programming by tapping the reader with your phone
- Any NFC tag can be used as a user identifier
- Supports opening door using NFC mobile phones
- History for latest 1000 events
- Cheap and easy solution

The PATRON-PRO system is designed primarily for the requirements of residential building, family houses, small offices and flats, where the system enables the owner to update user rights quickly and easily whenever needed just by tapping the phone at the reader. The

communication between the phone and the reader is carried out using NFC technology. The system also integrates an NFCporter function that enables users to identify themselves using a mobile phone with NFC.

The following figure shows the market growth of mobile access control systems in IMA in past three years. In last two years the sale of products doubled.

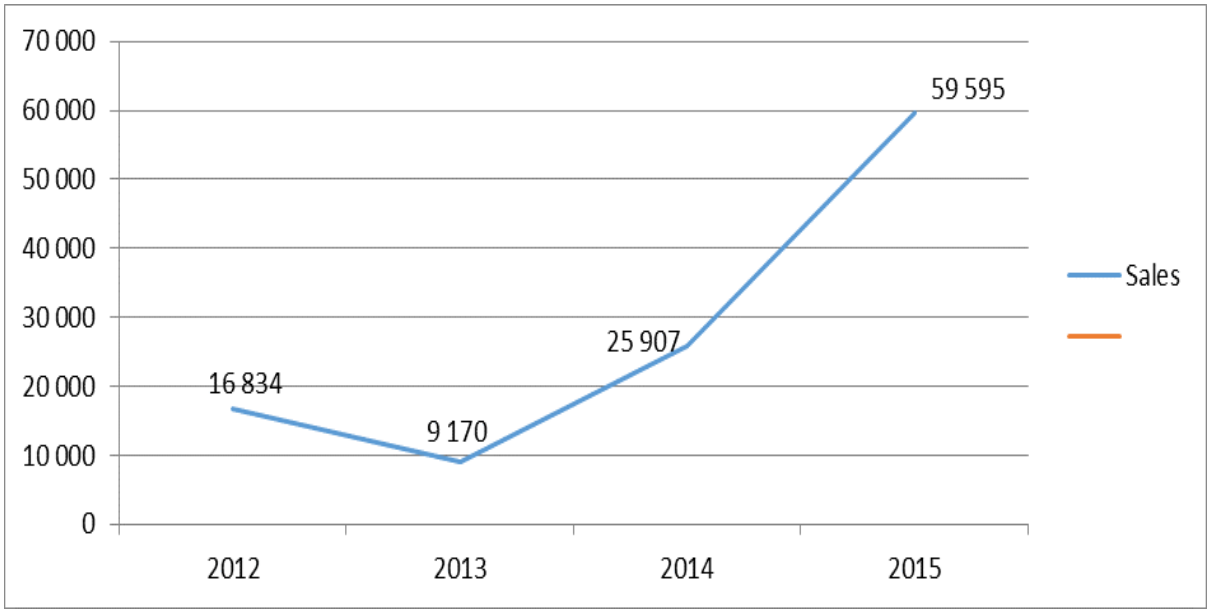


Figure 14: Sales of NFCporter, PATRON in IMA, 2012 – 2015 (till May), in Euro

Current Marketing strategies

Access control system PATRON-PRO is aimed at apartment houses and small sites including offices, family houses, flats etc. All marketing activities in this area are designed to answer the needs of users searching for solution to their problem at the right place and the right time.

We focus on cooperation with facility management companies, technology suppliers to apartment houses, door manufacturers and specialized shops. Second branch of our marketing activities is online advertising and support. We run PPC campaigns in major search engines and cooperate with professional servers advising local house managers and caretakers. All our activities are built around and directed to our website patron-pro.cz. On this website, prospective buyers can find all desired information and get in personal contact with our sales representative who finds a proper solution for them and guides them through the ordering process.

NFCporter system is aimed mainly on system integrators and larger companies seeking a solution for enhancing current RFID-based identification to utilize mobile phones as personal identifiers. The NFCporter system is designed for easy integration into current identification systems. In our marketing strategies we concentrate on presenting the strengths and innovations this system brings to corporate users. The reach of NFCporter system is worldwide and carried out solely online. We are running a microsite NFCporter.com and preparing press releases to be published by major professional servers. At the same time we are concentrating on building a strong SEO of our site to be easily accessible through search engines.

3.1.1.2 MATTHEW Implementation and future plan

Now, for both systems above, the ID is stored inside mobile phone data space. This is not very secure because if somebody who have deep knowledge of the system can copy application and data to the other mobile phone. When we will use MATTHEW microSD card or SIM with CIPURSE applet, security will be strongly increased. For enhancing of security the CIPURSE SAM can be used. We must only add SAM slot into the reader and update firmware, than the reader will be ready to work with high system security.

Matthew security concept using CIPURSE scheme and SAM can be directly used at IMA applications for enhancing of the security.

Nowadays IMA builds its application on CIPURSE Applet complying with T-Mobile SIM with data for simple identification, chained identification and for authentication with PIN. PIN application on Android Mobile platform already runs. As a SAM module IMA uses native application on the Infineon card for CIPURSE crypto rules calculation. When SIM&SAM pairing process is debugged and completed IMA will also complete personalization process on native SAM for INFINEON using proper Keys and T- mobile SIM Applets. Validation tests are to be performed by the end of June on the mobile where SIM will be simulated by HCE mobile. If it runs, new Applet for the SIM will be developed. We are going to use CIPURSE scheme for Access Control Systems in cooperation with T-Mobile. T-Mobile is to use own infrastructure to distribute the CIPURSE identifiers to the SIM.

3.2 Individual Exploitation Plans

While the section above outlined a general market overview, in the following, all partners state their updated, individual exploitation plans. Thereby, we take Recommendation 6 of the first annual review into account, which explicitly asked for detailed individual partner exploitation plans.

Partner 1 and 5: IFAT/IFAG Already at the beginning of the project it was internally elaborated, which results of the MATTHEW project will have the largest potential for exploitation. This evaluation is updated in regular re-spins and in close connection with customers like GTO or IMA and industrial partners along the value chain like AMS, CRX and TEC. Since Infineon Technologies as a hardware security anchor provider is interested in the various flavours of secure elements present on mobile platforms in the MATTHEW architecture the sales and marketing departments are in close contact with customers all around the globe.

This flexible approach allows Infineon on the one hand to support IMA with CIPURSE-based HW security anchors and push the integration technology to the smallest form-factors like nanoSIM, as they are requested by customers in the HW-based security markets. On the other hand Infineon is prepared as well to go towards new form factors, as proposed by GTO in terms of wearable devices with payment capabilities.

The outlook on the payment markets shows, that with the technologies researched in MATTHEW the future payment applications can be addressed not only in classical styles like card form factors with RFID-power supply, but also in battery powered wearable devices with versatile connectivity.

Just recently Infineon could prove its capabilities to address the hardware based security ICs markets by showing its Chipcard and Security ICs division growing by 50% in revenue YoY (from 121 mEUR in FQ2-2014 to 182 mEUR in FQ2-2015).

Partner 2: The work done with the MATTHEW project partners allowed **GTO** to optimize the design of its contactless microSDTM. Due to the market evolution and the forecast of new market opportunities, **GTO** has to identify a new form factor for the integration of the elements developed in the project. **GTO** has decided to switch to a System in Package

contactless front end that can easily be integrated in different devices, from IoT to wearables, to get an efficient contactless interface. This new technology brick will allow **GTO** to leverage on its existing product portfolio on secure and remote management server adapting them to the upcoming and promising market that is the IoT and Wearable with a smooth migration plan.

Partner 3: AMS planned to enable new opportunity in the RFID market for active transmission technology based system. In that sense is looking for new business partner and business case. As market leader in NFC active transmission technology based technology, new AMS partner and customer will be able to enhanced RF performance and reduced cost of integration and ownership of their NFC systems.

AMS is bringing research activities from other project together in particular: wearable and Wireless Sense together with NFC with the aim to enlarge its portfolio of systems and modules for RFID. AMS is working on new generation of NFC technology that enables mobile phones and wearable devices to emulate contactless cards reliably. This approach will enforce AMS leading position among IC suppliers of this market.

Partner 4: The companies behind most other partners are financed via products or services they provide. The Institute of Applied Information Processing and Communications (**IAIK**) is part of the Graz University of Technology and therefore not directly involved in many products or services. The role of IAIK is to research fundamental technologies to enable future products or services.

Nevertheless, the Graz University of Technology has its own Technology Exploitation Office (TEO) in order to make use of the §106 UG 2002 enabling the university to fulfil its mission to secure proper transfer of its intellectual property to industry. Services of the TEO include support of scientists from IAIK by information, education, and training concerning e.g. patent research and IP basics. Furthermore, ideas, proposals, manuscripts etc. are preliminary checked for commercial opportunities. Based on guidelines, it is the duty of each scientist to disclose inventions that are audited for legal, technical and economic criteria resulting in a SWOT analysis. If the analysis recommends commercialization strategies for protection and commercial exploitation are developed and executed by the TEO in close co-operation with the inventors and the institutes. Commercialization routes considered are licensing or selling of patents and know-how, value creation within spin-offs or start-ups and holding of strategic patents for attracting new businesses generating third-party money.

For the project, we assume that patent/utility-patent protection of cryptographic modules or optimization methods for implementations is possible. We expect to obtain patents that are independent from existing rights of third parties and we therefore do not expect to license rights of third parties for use of our invention.

Partner 6: TEC: Already after the first year the reputation gained from the project has positively influenced our acquisition activities. On top on the workflow based management support we provide on for cooperative research efforts on national and European level, we could make a first step to establish security engineering services, leveraging the knowledge gained from the work on hardware entangled security in the MATTHEW project. Being the main responsible partner for the work on PUF technology allowed us to sustainably steer the discussions and research directions in this application area. This positively influenced our internal developments and knowledge creation. Further the project experience triggered improvements of our IT framework, the so called “Trusted knowledge Suite”. We received value feedback from the partners and external experts which allowed us to enhance our services and appearance. The novelties introduced will further elevate the market position of this IT tool. As the national representative of the European Women in Science, Engineering and Technology (WiTEC) network Technikon we are using the project to promote the objectives of WiTEC.

Partner 7: IMA fulfils its original plan to make ready a generation of NFC subsystem components on top of IDSIMA4 platform. Taking present MATTHEW outcomes the new SW

application and component prototypes are available (new NFC reader, Android App) and these are in process of testing. Continuing by converting MATTHEW outcomes to new prototypes will help IMA to expand its portfolio of the new NFC components. IMA already presents new concepts of applications to current significant customers and new marketing processes are taken place. Very first feedbacks indicate that access control systems enriched by new security concept described in three IMA's use cases are very promising.
Partner 8: CRX intends to promote the technological outcomes of MATTHEW by enriching its software offer with cryptographic libraries supporting the privacy-protection mechanisms conceived within the project. The cryptographic technologies subject to exploitation fall in the category of PETs (Privacy-Enhancing Technologies) and will support anonymous signatures and attribute-based credentials, which are on the rise in privacy-friendly cloud applications. The most appropriate security marketplace for these technologies is the one of pervasive end-user or corporate applications that preserve user privacy while enabling access to online services. The technology is to be co-owned by the partners and protected by patents as appropriate.

Chapter 4 Conclusion

This document summarizes the progress of dissemination and exploitation activities of the MATTHEW project within the first one-and-a-half years. The dissemination stakeholders were identified, in order to address the different stakeholder groups by promoting the applicable dissemination activities of the MATTHEW partners. A homepage and a visual identity have been designed and are freely accessible. Several publications have been made and therefore already much of the ongoing research was disseminated within the community.

Further, a market analysis has been performed, to assure that the MATTHEW research goals are still market relevant. Based on that new developments and insights the exploitation plans of all partners have been updated.

Therefore, the MATTHEW consortium is fully prepared for the following one-and-a-half years of research, dissemination, and exploitation.

Chapter 5 List of Abbreviations

ACL	Access Control List
BYOD	Bring your own Device
CMS	Content Management System
ECC	Elliptic Curve Cryptographic
HCE	Host Card Emulation
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
MNO	Mobile Network Operator
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
OTT	Over the top
SSL	Secure Sockets Layer
SVN	Subversion
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol

Table 4: List of Abbreviations