CHIST-ERA

User empowerment for SEcurity and privacy in Internet of Things

Report on Y1 outreach activities and Y2 planning

Deliverable number: D5.1

Version 1.0

Funded by the Future and Emerging Technologies (FET) CHIST-ERA programme of the European Union.

Project Acronym:	USEIT
Project Full Title:	User empowerment for SEcurity and privacy in Internet of Things
Call:	2015
Grant Number:	20CH21_167531
Project URL:	http://useit.eu.org

Editor:	Antonio Skarmeta, Universidad de Murcia (UMU) – Spain
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Delivery Date:	2018-01-31
Authors:	José Luis Hernández Ramos, University of Murcia Salvador Pérez Franco, University of Murcia Antonio Skarmeta, University of Murcia
Peer review:	Jan Camenisch, IBM Research – Zurich

This document provides an overview of Y1 outreach activities and Y2 planning proposal. The deliverable describe who the project organises the transfer of knowledge and project results to the outside world, as well as within the consortium. It describes how USEIT informs and promotes project results to the stakeholder communities. Of particular importance will be articles, papers for journals and conferences, or other publicity

The deliverable objectives are:

- To drive the effort of disseminating project activities and findings and to create impact
- Provide scientific outcomes via conference and journal publications
- To provide an outreach strategy focused on society and stakeholders

Contents

List of Figures

List of Tables

1. USEIT dissemination strategy plan

In order to achieve the dissemination and exploitation of the USEIT project's results, the partners will adopt a dissemination plan which aims at establishing strong communication channels with the target audience. The proposed plan will provide guidelines on communicating the project's vision and results, with recognizable, clear and effective messages, as well as stimulate interest in the project technologies and achievements.

1.1. Expected Impact

Impact on Science and Technology

One of the main objectives of USEIT is to improve the security and privacy of interacting IoT devices, and especially to put the user in the center of the security and privacy configuration. The project will provide novel algorithms and tools that are optimized for IoT use cases, so that security and efficiency no longer have to be contradictory requirements. USEIT tools will result from extensive evaluation and, more importantly, from validation mechanisms based on user intuition of security and privacy concepts through a multidisciplinary approach that will be taken within the co-creation workshops. Users will be able to control the complexity and scalability of IoT by offering a simple way to configure and monitor data access and policy compliance. All results of the project will be published and made available open-source as much as possible, enabling easy adoption by external stakeholders.

Standardization

To facilitate the adoption of USEIT technologies, the project will actively contribute to relevant standardization bodies. The participation will include tracking relevant innovations, contributing to standardization documents and processes in relevant fields, as well as providing new proposed standards. Specific standardisation organisations and the expected contributions include: the Kantara Initiative, especially for their User-Managed Access (UMA) protocol; IETF, in relation to the WG ACE Authentication and Authorization for Constrained Environments; IEEE IoT Initiative related to the educational program on IoT; ETSI, which published several standards related to European vehicle communication; W3C, which originally published the enterprise privacy policy language EPAL and is now defining formats for Verifiable Claim and Anonymous Credentials; OASIS, where USEIT could contribute to the access control language XACML; or the FIDO alliance, for which partner IBM has made an authenticate specification based on the direct anonymous attestation protocol (which is very relevant for USEIT as well).

Increasing awareness

USEIT will also contribute towards the Europe 2020 Strategy [1] in the area of user-centric security and make a convincing case that also in IoT, privacy and security can indeed go together. USEIT will provide a dashboard to let users handle their policy for security and privacy in a secure and convenient way. Moreover, USEIT also considers current trends of technology usage by users such as the increasing use of smart object by citizens, and in general for different kind of M2M communications. This approach will in turn help bridge the technological gap between most citizens and ICT.

Reducing social barriers

The USEIT prototypes will empower users to benefit from the advantages of technology to protect their information, thereby breaking the technological gap of most citizens to ICT. In terms of social transformation factors, USEIT will contribute to reduce several barriers, including end-user acceptance by providing a secured and privacy-by-design solution in line with the end-users' requirements and by increasing the users' acceptance and satisfaction. Users will feel more secure in the interaction with IoT, smart objects and Smart Cities in general. The result will be fewer negative experiences, which at the end will increase the trust in the use of IoT by EU citizens and businesses.

Sustainability

The USEIT platform may be deployed in regional Smart City Plans such as that of Lorca City and Murcia City, which could help securing future funding as part of the regional ERDF based on the *Smart Specialisation Strategy*.

1.2. Dissemination Strategy Description

The USEIT dissemination plan consists of different phases and is based on an iterative process to improve its effectiveness during the project timespan. The overall view of the dissemination plan is provided in Figure 1.1.

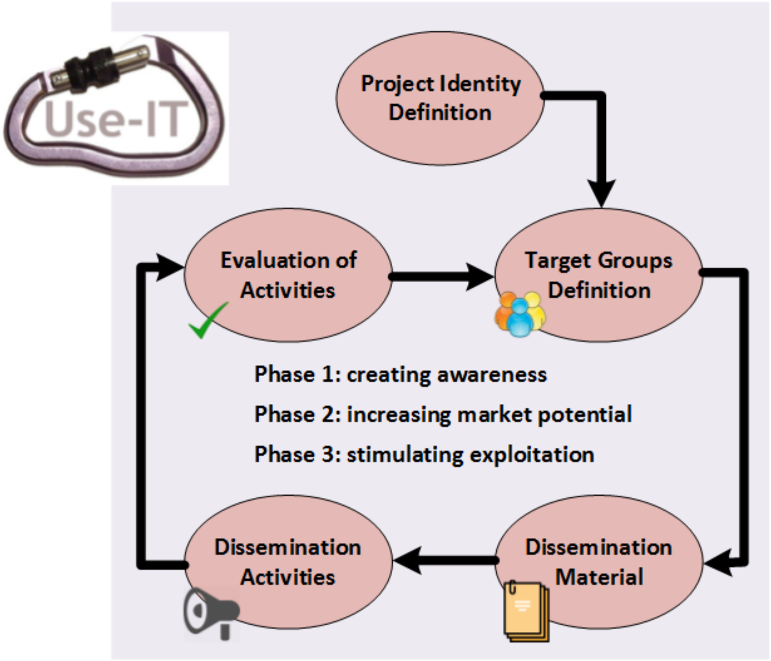

Use-IT
Project Identity Definition
Evaluation of Activities
Target Groups Definition
Phase 1: creating awareness
Phase 2: increasing market potential
Phase 3: stimulating exploitation
Dissemination Activities
Dissemination Material

Figure 1.1: Overall view of the USEIT dissemination plan

The following phases are envisioned in the USEIT dissemination plan:

- **Project identity definition.** The partners intend to provide recognizable, clear and effective messages that communicate the project vision and results, as well as stimulate interest in the project technology and results. This will be pursued by defining a project "logo", including "advertising slogans", common graphical layout and look-and-feel for all dissemination material, a list of keywords and basic concepts on which to base all communication actions.

- **Target groups' definition.** The project dissemination will be tailored to the target audience, mainly public at large, the research community and potential third parties interested to use the outcomes of the project, including public administrations, SMEs and industry.
- **Dissemination material.** A broad range of dissemination material will be developed: general presentation material (such as project brochures and leaflets), and PowerPoint presentations; more specific presentations such as technology descriptions, industrial cases description, proceedings of workshops; demonstrators, such as on line software, videos, and downloadable software demonstrators.
- **Selection of the appropriate dissemination activities.** Dissemination activities are essential for any research project and must address the selected target groups in order to maximize the impact of project dissemination. A set of generic/common instruments will be used in order to engage more efficiently with all stakeholders groups and to maximize its outreach with different audiences, as summarized Table 1.1.
- **Evaluation of dissemination activities performed.** Feedback, for each dissemination activity, will be collected including qualitative and quantitative information (number of participants, cultural background, contact established, comments and suggestions) and will be analysed to derive indications used to improve the dissemination activities. If possible, evaluation tools, such as electronic forms and questionnaires, will be adopted.

Table 1.1: Dissemination activities based on target groups' definition

Target Group	Technical level	Main focus	Dissemination activities
Public / Citizens	Understandable by a large public of non-specialists	General project presentation Economic impact and societal benefits Personal data protection	Project website Social medias Media
Research Community	High level on the scientific and technical innovation	Specific project presentation Scientific innovation	Conferences Publications Specialized networks/fora Project website Social medias / twits
Industry, SMEs and public administrations	Focus on the technology enablers and potential economic exploitation and societal benefits	Standarization Scientific and technical innovations Business opportunities Societal benefits	Direct contacts Conferences and fairs Publications Project website Standards

The project will exploit different communication channels to carry out the dissemination activities and maximize its outreach with different audiences. In Table 1.2, we report a list of envisioned dissemination activities in the USEIT project. This list can be updated and extended in the next phases of the project.

Scientific Publications: USEIT intends to disseminate its innovation results in international peer reviewed scientific journals, magazines, book chapters and conferences. The editorship of book and chapters related to the project research items will be also exploited as a means to externalise USEIT work and to document the advances with reference to the state-of-the-art achievements. Target journals are detailed in the annex.

Contributions and participation at international conferences, workshops and summits: The projects results will be also disseminated at conferences, foras, SDO and bodies that are attended by potential future users. The project will also submit and present papers in selected, highly recognized international conferences and workshops. See annex.

Website: A comprehensive public website that will contain all relevant information about the project. It will give provide a centralized access to the various publicly available deliverables, publications and articles related to the project. The site will be regularly updated over the lifetime of the project with the project publications

Table 1.2: List of dissemination activities

Dissemination Activity Type
Scientific Publications
Contributions and participation at international conferences, workshops and summits
Website
Social networks presence
Brochure, flyer and printed materials
Participation in Summer schools from ITN and other projects
Other

and public materials, such as flyers, posters and public deliverables, organized workshops, available services, etc.

Social networks presence: The project intends to develop its presence on the social networks, such as LinkedIn, Twitter and Facebook. The first two channels will be used for interaction with more professional community (researchers, SMEs, large industry), while the latter will be used for interaction with the general public (while being cautious with the personal data protection issue).

Brochure, flyer and printed materials: The project will prepare appropriate printed materials like leaflets to promote the project's outcomes to the general public, as well as press releases, and other medias through the strong communication offices of the partners.

Participation in Summer schools from ITN and other projects: Open to students/researchers will serve to increase the interaction of the project partners with students and research groups at UE level and will serve as an outreach channel of the project activities.

Objectives KPI for project dissemination:

- International Impact Journals > 6
- International Conferences > 11
- Workshop and Summer Schools participation > 4

Furthermore, it should be pointed out that statistics of publications, the number of citations, submitted standard proposals, as well as the number of website visitors and reference links will be continuously collected serving as a performance metric.

2. Initial USEIT dissemination activities

To guarantee a wide spread of project results as well as well as to ensure a maximum impact, different dissemination activities will be carried out during the whole project lifespan of the USEIT project. Accordingly, we provide an overview of these initial dissemination activities being carrying out in the project: logo, website and scientific publications.

2.1. USEIT logo

The project logo defines the project visual identity, creates an easily recognizable "image" and helps to improve the visibility. It should be used prominently in all dissemination tools and printed materials. Figure 2.1 shows the USEIT logo.

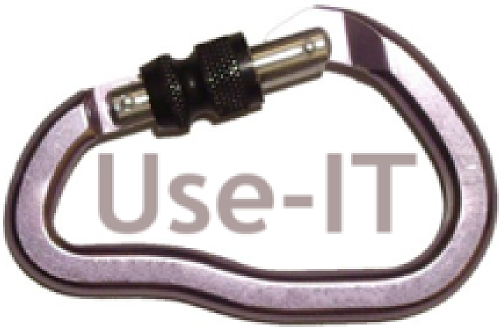
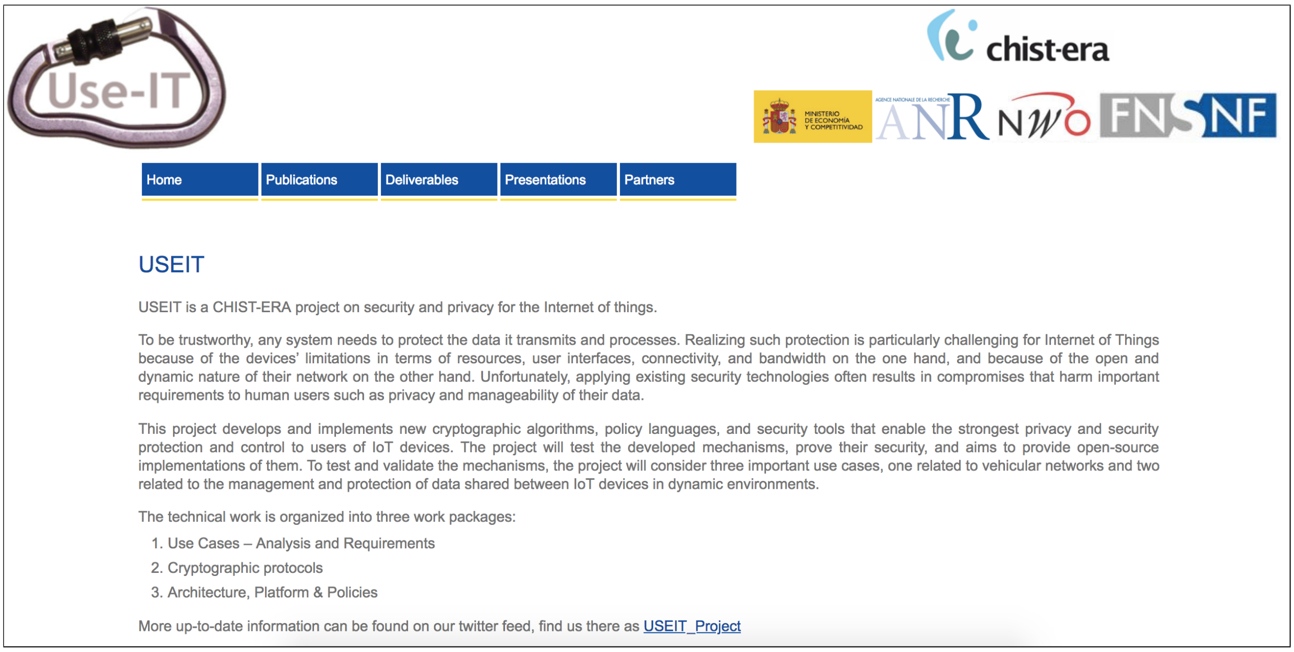


Figure 2.1: USEIT logo

2.2. USEIT website

The USEIT website is available under the URL useit.eu.org and it is composed of the following main sections: Publications, Deliverables, Presentations and Partners. It should be pointed out that, in this sections, the corresponding documents related to this project will be uploaded to this website. Figure 2.2 shows the screenshots of the USEIT website.



USEIT

USEIT is a CHIST-ERA project on security and privacy for the Internet of things.

To be trustworthy, any system needs to protect the data it transmits and processes. Realizing such protection is particularly challenging for Internet of Things because of the devices' limitations in terms of resources, user interfaces, connectivity, and bandwidth on the one hand, and because of the open and dynamic nature of their network on the other hand. Unfortunately, applying existing security technologies often results in compromises that harm important requirements to human users such as privacy and manageability of their data.

This project develops and implements new cryptographic algorithms, policy languages, and security tools that enable the strongest privacy and security protection and control to users of IoT devices. The project will test the developed mechanisms, prove their security, and aims to provide open-source implementations of them. To test and validate the mechanisms, the project will consider three important use cases, one related to vehicular networks and two related to the management and protection of data shared between IoT devices in dynamic environments.

The technical work is organized into three work packages:

1. Use Cases – Analysis and Requirements
2. Cryptographic protocols
3. Architecture, Platform & Policies

More up-to-date information can be found on our twitter feed, find us there as USEIT_Project

Figure 2.2: USEIT website

2.3. Publications

The publications carried out in the scope of USEIT project include 12 conference papers and 2 journal papers. Details on these publications are reported in Table 2.1.

Table 2.1: Scientific publications related to the USEIT project

Title	Type	Authors	International	Partners
A lightweight and flexible encryption scheme to protect sensitive data in Smart Building scenarios IEEE Access, vol. PP, no.99, 2018 https://doi.org/10.1109/ACCESS.2018.2801383	Journal Paper	Salvador Perez Jose L. Hernandez-Ramos Sara N. Matheu-Garcia Domenico Rotondi Antonio F. Skarmeta Leonardo Straniero Diego Pedone	Yes	UMU
Systematic literature review on the state of the art and future research work in anonymous communications systems Computers & Electrical Engineering. In press. https://doi.org/10.1016/j.compeleceng.2017.11.027	Journal Paper	Mehran Alidoost Nia Antonio Ruiz-Martínez	Yes	UMU
Integrating LP-WAN Communications within the Vehicular Ecosystem The 2017 International Symposium on Mobile Internet Security (Mobisec 2017)	Conference	R. Sanchez-Iborra J. Sanchez-Gomez J. Santa P.J. Fernandez A. Skarmeta	Yes	UMU
IPv6 Communications over LoRa for Future IoV Services IEEE 4th World Forum on Internet of Things (WF-IoT). Singapore, 2018. To appear	Conference	Ramon Sanchez-Iborra Jesus Sánchez-Gómez José Santa Pedro J. Fernández Antonio F. Skarmeta	Yes	UMU
Test-based Risk Assessment and Security Certification Proposal for the Internet of Things IEEE 4th World Forum on Internet of Things (WF-IoT). Singapore, 2018. To appear	Conference	Sara Nieves Matheu Garcia José Luis Hernández-Ramos Antonio Skarmeta	Yes	UMU
Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain ACM CCS 2017: 683-699	Conference	Jan Camenisch Manu Drijvers Maria Dubovitskaya	Yes	IBM
Privacy-preserving attribute-based credentials in cooperative intelligent transport systems IEEE VNC 2017: 131-138	Conference	Gregory Neven Gianmarco Baldini Jan Camenisch Ricardo Neisse	Yes	IBM
Anonymous Attestation with Subverted TPMs CRYPTO 2017: 427-461	Conference	Jan Camenisch Manu Drijvers Anja Lehmann	Yes	IBM
One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation In IEEE Symposium on Security and Privacy 2017: 901-920	Conference	Jan Camenisch Liqun Chen Manu Drijvers Anja Lehmann David Novick Rainer Urian	Yes	IBM
UC-Secure Non-Interactive Public-Key Encryption In CSF 2017: 217-233	Conference	Jan Camenisch Anja Lehmann Gregory Neven Kai Samelin	Yes	IBM
Accumulators with Applications to Anonymity-Preserving Revocation In EuroS&P 2017: 301-315	Conference	Foteini Baldimtsi Jan Camenisch Maria Dubovitskaya Anna Lysyanskaya Leonid Reyzin Kai Samelin Sophia Yakoubov	Yes	IBM
One-Shot Verifiable Encryption from Lattices In EUROCRYPT 2017: 293-323	Conference	Vadim Lyubashevsky Gregory Neven	Yes	IBM
Privacy-Preserving User-Auditable Pseudonym Systems In EuroS&P 2017: 269-284	Conference	Jan Camenisch Anja Lehmann	Yes	IBM
Reinforcing IoT-Enforced Security Policies TrustCom 2018	Conference	Nouha Oualha	Yes	CEA

2.4. Other dissemination activities

Project participants have given a number of talks that presented project results:

- Jan Camenisch, A Decade of Direct Anonymous Attestation, IMA Conference on Cryptography and Coding, Invited Talk, Oxford, 2017-12-13.
- Jan Camenisch, Directions for Security Research, ICETE 2017 and SECRYPT 2017, Joint Keynote, Madrid, 2017-07-24.
- Jan Camenisch, Anonymous Credentials and e-Cash, Cybersecurity and Privacy - EIT Digital Infrastructure Summer School, Lecture, Trento, 2017-07-04.
- Jan Camenisch, Secure Digital Identities, Techdays Munich, Munich, 2017-06-23.
- Jan Camenisch, Direct Anonymous Attestation - From 2003 to 2017 and Beyond, CySeP Summer School, Lecture, KTH, Stockholm, How to build privacy-protecting cryptographic protocols, 2017-06-21.
- Jan Camenisch, Mathematical Institute, Cryptography Seminar, Oxford University, 2017-06-07.
- Jan Camenisch, Authentication without Identification - Data protection for IoT, IoT Week, Keynote, Geneva, 2017-06-06.
- Jan Camenisch, Cryptography 4 People (Where we should be heading), IFIP Sec 2017, Keynote, Rome, 2017-05-29.
- Jan Camenisch, Cryptography 4 People, Universidad Autónoma de Madrid , Security Seminar, Lecture, Madrid, 2017-04-03.
- Jan Camenisch, (Un)linkable identifiers for distributed databases (Crypto 4 People - databases), ZISC Lunch Seminar, ETH Zurich, Lecture, Zurich, 2017-03-15.
- Gregory, ESCAR.

Interaction with standardization bodies and similar groups:

- CITS platform.
- W3C Credentials and Verifiable Claims working group. These standardize formats for (privacy-friendly) exchange of personal information.
- FIDO (fast identity online). We have worked with members from the FIDO alliance to propose protocols for privacy-protecting on-line authentication with mobile devices. The protocols also extend to authentication in IoT scenarios. Together we are currently investigating extensions to the proposed protocols to improve privacy in further IoT scenarios.

The project has engaged in interactions with the following individuals who have a strong influence in the area of vehicular communication infrastructures:

- Gianmarco Baldini (JRC Ispra).
- William White (Security Innovation), strong influence on the solutions discussed in the US.
- Matthew Green (Johns Hopkins University)[1]
- Anna Lysanysya (Brown University) & Leo Reyzin (Boston University)[2]
- Jan Camenisch, Secure Digital Identities, Techdays Munich, Munich, 2017-06-23.
- Jan Camenisch, Secure Digital Identities, Techdays Munich, Munich, 2017-06-23.

Contact with ESCAR workshop:

- The project had presented itself at the ESCAR 2017 conference in Berlin (Invited talk by Gregory Neven).

[1] https://blog.cryptographyengineering.com

[2] https://freedom-to-tinker.com/2017/06/21/killing-car-privacy-by-federal-mandate/

- For ESCAR 2018 (Brussels), the project aims to present the current project results. Also, we will organize a stakeholder workshop in conjunction with the conference to 1) discuss in detail the project results but also state-of-the-art technologies for CITS solution in general and 2) to gather directions and opinions of stakeholders from the car manufacturer. In fact, it has turned out at ESCAR 2017 that many stakeholders from car manufacturer are not aware of what currently happens in the area of CITS and of the related state of the art in the scientific literature.

2.5. Y2 activities

During Y2 USEIT will increase it dissemination and outreach activities once the main components ad architecture definition are already in place.

As indicated one of the main aspects to be carried out it is related to the launching of the communities engagement activities and that will support the finalization of D1.2. Possible users and communities that will be involved to get enough and more precise feedback are:

- Car manufacturers: this will be done also with a workshop at ESCAR 2018.
- Smart building: building managers, building users at U. Murcia, using questionnaires and mock-ups.
- Developer communities: targeting different possible communities as Raspberry Pi, or ARM developers using the network of collaboration already exiting between partners.

In that sense within Y2:

- A workshop collocated with ESCAR conference will be scheduled where also an advisory board meeting will be scheduled.
- Participation on CHISTERA workshop Paris 11-12 April 2018.
- Contribution to the EIT Digital Summer School in Privacy, Security & Trust, held at CLC Trento.
- Participation in IoTWeek Bilbao 4-6 June 2018 in the panel on Security and Privacy for IoT.
- Contributions to the standardization activities in fora likes W3C policy claims, FIDO and IETF.
- Continue the contribution to the Stakeholder workshop C-ITS.

Bibliography

[1] E. C. (EC), “Europe 2020: a strategy for smart, sustainable and inclusive growth,” 2010. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

A. Annex

Scientific Publications: USEIT intends to disseminate its innovation results in international peer reviewed scientific journals, magazines, book chapters and conferences. The editorship of book and chapters related to the project research items will be also exploited as a means to externalise USEIT work and to document the advances with reference to the state-of-the-art achievements. Target journals are: IEEE Pervasive Computing Magazine[1], Springer Personal and Ubiquitous Computing[2], IEEE Communication Magazine[3], IEEE Security & Privacy[4], Elsevier Journal of Parallel and Distributed Computing[5], Elsevier Journal of Systems and Software[6], Elsevier Computer Communications[7], Elsevier Ad-Hoc Networks[8], International Journal of Product Development[9], International Journal of Entrepreneurship and Innovation Management[10]. Also to mention that partners are already associated editor of journals like Elsevier Computer Networks[11], IEEE Transactions on Computers[12], IEEE Transactions on Systems, Man, and Cybernetics[13], J. Of Cryptographic Engineering., and other like Wiley Security and Communication Networks[14], that will provide possible journals to look for a Special Issue related to the project results.

Contributions and participation at international conferences, workshops and summits: The projects results will be also disseminated at conferences, foras and bodies which are attended by potential future users. One example is the Industry 4.0 platform established in Germany to push the fourth industrial revolution. The project will also submit and present papers in selected, highly recognized international conferences and workshops, such as: ACM Conference on Computer and Communications Security[15], IFIP International Information Security and Privacy Conference[16], IEEE International Conference on Internet of Things[17], IEEE International Conference on Distributed Computing in Sensor Systems[18], ACM International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems[19], IEEE Pervasive Computing and Communication[20] conference, IEEE International Parallel & Distributed Processing Symposium[21], ACM Symposium on Access Control Models and Technologies[22], International Symposium on Algorithms for Sensor Systems, Wireless Ad Hoc Networks and Autonomous Mobile Entities[23], etc. The project will also participate in the workshops organized by the European Commission, CHIST-ERA, IERC, and other relevant organizations like the IoT Forum,

[1] http://www.computer.org/portal/web/pervasive
[2] http://link.springer.com/journal/779
[3] http://www.comsoc.org/commag
[4] http://www.computer.org/portal/web/security
[5] http://www.journals.elsevier.com/journal-of-parallel-and-distributed-computing/
[6] http://www.journals.elsevier.com/journal-of-systems-and-software/
[7] http://www.journals.elsevier.com/computer-communications/
[8] http://www.journals.elsevier.com/ad-hoc-networks/
[9] http://www.inderscience.com/jhome.php?jcode=ijpd
[10] http://www.inderscience.com/info/inarticletoc.php?jcode=ijeim
[11] http://www.journals.elsevier.com/computer-networks/
[12] http://www.computer.org/portal/web/tc
[13] http://www.ieeesmc.org/publications/
[14] http://onlinelibrary.wiley.com/journal/10.1002/%28ISSN%291939-0122
[15] http://www.sigsac.org/ccs.html
[16] http://www.sec2013.org/
[17] http://www.china-iot.net/iThings2013.htm
[18] http://www.dcoss.org
[19] http://mswimconf.com
[20] http://www.percom.org/
[21] http://www.ipdps.org/
[22] http://www.sacmat.org/2013/index.php
[23] http://www.algosensors.org/

CHES, FDTC, PKC, COSADE, DATE, RFIDSec.