| | |
|---|---|
| Project Title | Trust-aware, Reliable and Distributed Information Security in the Cloud |
| Project Acronym | TREDISEC |
| Project No | 644412 |
| Instrument | Research and Innovation Action |
| Thematic Priority | Cybersecurity, Trustworthy ICT |
| Start Date of Project | 01.04.2015 |
| Duration of Project | 36 Months |
| Project Website | www.tredisec.eu |

# <D7.2: DISSEMINATION PLAN>

| | |
|---|---|
| Work Package | WP7 Communication, Dissemination and Exploitation |
| Lead Author (Org) | Melek Önen (EURECOM) |
| Contributing Author(s) (Org) | All partners |
| Reviewers | David Vallejo (ARSYS), Elena García (ATOS), Jose F. Ruíz (ATOS) |
| Due Date | M6 |
| Date | 30.09.2015 |
| Version | 4.1 |

Dissemination Level

| | |
|---|---|
| X | PU: Public |
| | CO: Confidential, only for members of the consortium (including the Commission) |

# Versioning and contribution history

| Version | Date | Author | Notes |
|---------|------|--------|-------|
| 0.1 | 21.07.2015 | Melek Önen (EURECOM) | First outline |
| 0.2 | 24.08.2015 | Melek Önen (EURECOM) | Draft version |
| 1.0 | 28.08.2015 | Melek Önen (EURECOM) | First version to be internally reviewed. |
| 1.1 | 14.09.2015 | David Vallejo (ARSYS), Elena González (Atos) | Review provided. |
| 2.0 | 15.09.2015 | Melek Önen (EURECOM) | Second version, which addresses reviewer's comments. |
| 3.0 | 15.09.2015 | Melek Önen (EURECOM) | Third version waiting for approval |
| 3.1 | 22.09.2015 | Jose Ruiz (Atos) | Reviews provided |
| 4.0 | 23.09.2015 | Melek Önen (EURECOM) | Final version |
| 4.1 | 28.09.2015 | Beatriz Gallego-Nicasio Crespo (ATOS) | Quality Check |

# Disclaimer

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

# Table of Contents

# List of Tables

# Executive Summary

This document sets out the initial plan to raise awareness of the TREDISEC project concepts and solutions. In this plan, we only outline the scientific dissemination activities whereas all remaining communication activities are described in deliverable D7.3 "Communication Strategy and Plan".

The dissemination strategy defines the way TREDISEC will engage different dissemination groups including academic researchers and business stakeholders. These target communities will be reached through appropriate channels throughout the lifetime of the project. Once target communities are built the plan distinguishes between means for maintaining general awareness with respect to the project concept and research results and those means for engaging business communities towards the third year of the project.

In order to maximize the visibility of the project outcomes, a list of potential activities and partners' already planned activities are finally detailed in the document.

# 1 Introduction

## 1.1 Objectives of the dissemination activity

The broad aim of TREDISEC dissemination activities is to spread technological achievements and knowledge of the project both to the research and academic environment as well as to the business community. These activities will also be supported by communication activities targeting a wider range of stakeholders (cf. deliverable D7.3). The TREDISEC consortium consists of highly skilled and experienced partners capable of disseminating project results to the targeted communities.

Dissemination will be continuous and the plan will evolve throughout the lifetime of the project. The WP7 work package adopts an iterative methodology with the following objectives:

- to identify the potential stakeholder groups for targeted dissemination activities;

- to raise awareness on the project scope among a wide range of stakeholders and support coordination of research and dissemination activities with parties outside the project;

- to encourage the adoption of the TREDISEC approach and continuously communicate the project's technical achievements and innovation results;

- to support the marked nature of the innovation of the project, and specifically its scientific/technical dimension defined in D1.5 "Innovation Strategy and Plan".

## 1.2 Document Outline

The deliverable is organized as follows:

- Section 2 defines who TREDISEC aims to reach.

- Section 3 identifies the various dissemination channels through which TREDISEC solutions will be communicated.

- Section 4 describes the project's dissemination plan defined by three phases.

- Section 5 finally lists current dissemination activities of TREDISEC partners.

# 2   TREDISEC target communities

## 2.1   Research Community

An important target group for scientific dissemination activities in TREDISEC is the research community including not only **universities, research centres and other academic institutions** but also **R&D departments of industrial companies**. TREDISEC aims at raising awareness of the privacy and security challenges specific to the cloud computing environment and of the recent advances on TREDISEC specific topics such as searchable encryption, storage and computation verifiability, access control and secure isolation.

Partners will further disseminate their project results to this community through **publications** and **participation and organization of some workshops**. These will foster the opportunity to coordinate and collaborate among different research groups. TREDISEC aims to approach the research community with different additional means which are described in section 3.

## 2.2   Business Community

The objective of the dissemination activities is to build interest in the TREDISEC results within the business community. TREDISEC aims at motivating this community including technical and business experts to take steps towards adopting/implementing TREDISEC solutions early in their business process.

TREDISEC industrial partners will first start to disseminate project results internally to their products/business units. Further, all TREDISEC partners will target industrial stakeholders to widely disseminate the project research results. This objective will ensure that the further exploitation and commercialisation potentials identified in deliverable D1.5 are maximised beyond the end of the project.

## 2.3   Other EU/national/international projects

TREDISEC partners are well positioned to engage with many initiatives with European, national and international research projects. Such collaborations will not only help to promote the scientific results of TREDISEC but they will also enlarge the visibility and application of the TREDISEC solutions to other contexts.

The list of the undergoing potential projects TREDISEC may collaborate with is provided in deliverable D7.3. TREDISEC partners will first start to raise awareness of the TREDISEC concept to the other projects they are involved in and further identify common challenges in order to foster collaboration among potential projects.

# 3   Dissemination channels

## 3.1   Publications

The main scientific dissemination activity for TREDISEC is the publication **of the innovative research results**: Partners will publish the results of the conducted research in relevant conferences and journals to maximize the impact of the scientific work to the target communities. The project targets top quality conferences and journals in order to obtain valuable feedback from the communities and produce high quality publications. Table 1 provides a list of relevant conferences and workshops not only in the field of cryptography and security but also in the more focused field of cloud security.

Furthermore, partners will also target referred journals listed in Table 2 to ensure the high visibility of their work.

Both Tables 1 and 2 will be regularly updated during the lifetime of the project and shared among partners.Additionally, these tables and the TREDISEC publications will also be announced in the project's official website presented in D7.3.

## 3.2   Talks, Training activities

TREDISEC partners will also participate in workshops or other events such as webinars or online courses not only to promote the research results but also to provide a solid background for young researchers in cloud security. In this sense, partners will be involved in different training workshops such as summer schools by giving talks on the different TREDISEC topics. A list of potential summer schools and training workshops is provided in Table 3.

## 3.3   Conference organization

In addition to the previously described dissemination channels, TREDISEC is also planning to organize scientific workshops during its lifetime in order to also participate in the gathering of targeted stakeholders. Thanks to these workshops, TREDISEC partners will not only have the chance to promote their own research activities but also to exploit other researchers' relevant results within TREDISEC.

Furthermore, the project is planning to produce a **final workshop** that will be held towards the end of the project aiming at presenting all the results acquired during the project widely and hence maximizing inputs also on exploitation issues.

| Conference/ Workshop Acronym | Conference Name | Dates & Location (if available) | Next Submission deadline (if not expired) |
|---|---|---|---|
| **IFIP SEC** | International Conference on ICT Systems Security and Privacy Protection | 30 May - 01 June 2015, Ghent, Belgium | expired; 2016 dates not available yet |
| **Cryptology** | International Cryptology and Information Security Conference | 31 May – 2 Jun 2015, Sabah, Malaysia | expired; 2016 dates not available yet |
| **SACMAT** | ACM Symposium on Access Control Models and Technologies | 1-3 Jun 2015, Vienna, Austria | expired; 2016 dates not available yet |
| **ACNS** | International Conference on Applied Cryptography and Network Security | 2-5 Jun 2015, New York, USA | expired; 2016 dates not available yet |
| **STOC** | Symposium on the Theory of Computing | 18-21 Jun 2015, Cambridge, USA | expired; 2016 dates not available yet |
| **Usenix Security** | USENIX Security Symposium | 12-14 Aug 2015, Washington D.C, USA | expired; 2016 dates not available yet |
| **TRUST** | International Conference on Trust & Trustworthy Computing | 24-26 Aug 2015, Heraklion, Greece | expired; 2016 dates not available yet |
| **ISC** | Information Security Conference | 9-11 Sep 2015, Trondheim, Norway | expired; 2016 dates not available yet |
| **DPM** | Data Privacy Management International Workshop | 21-22 Sep 2015, Vienna, Austria | expired; 2016 dates not available yet |
| **ESORICS** | European Symposium on Research in Computer Security | 21-25 Sep 2015, Vienna, Austria | expired; 2016 dates not available yet |
| **CNS** | IEEE Conference on Communications and Network Security | 28-30 Sep 2015, Florence, Italy | expired; 2016 dates not available yet |
| **SPC** | 1st Workshop on Security and Privacy in the Cloud | 30 Sep 2015, Florence Italy | expired; 2016 dates not available yet |
| **CCS** | ACM Conference on Computer and Communications | 12-16 Oct 2015, Denver, Colorado, USA | expired; 2016 dates not available yet |
| **Euro S&P** | IEEE European Symposium on Security and Privacy | 12-16 Oct 2015, Saarbrucken, Germany | expired; 2016 dates not available yet |
| **CCSW** | ACM Cloud Computing Security Workshop | 15 Oct 2015, Denver, Colorado, USA | expired; 2016 dates not available yet |
| **FPS** | Foundations and Practice of Security | 26-28 Oct 2015, Clermont-Ferrand, France | expired; 2016 dates not available yet |

| ICISC | Annual International Conference on Information Security and Cryptology | 25-27 Nov 2015, Seoul, Korea | expired; 2016 dates not available yet |
|---|---|---|---|
| ASIACRYPT | Annual International Conference on the Theory and Application of Cryptology | 29 Nov- 3 Dec 2015, Auckland, New Zealand | expired; 2016 dates not available yet |
| INDOCRYPT | INDOCRYPT | 6-10 Dec 2015, Bangalore, India | expired; 2016 dates not available yet |
| ACSAC | Annual Computer Security Applications Conference | 7-11 Dec 2015, Los Angeles, CA, USA | expired; 2016 dates not available yet |
| CANS | International Conference on Cryptology and Network Security | 8-12 Dec 2015, Marrakech, Morocco | expired; 2016 dates not available yet |
| TCC | IACR Theory of Cryptography Conference | 10-13 Jan 2016, Tel Aviv, Israel | expired; 2016 dates not available yet |
| NDSS | Network and Distributed System Security Symposium | 21-24 Feb 2016, San Diego, USA | expired; 2016 dates not available yet |
| Financial Crypto | Financial Cryptography and Data Security | 22-26 Feb 2016, Barbados, | 02 Oct 2015 |
| CT-RSA | RSA Conference Cryptographers' Track | 29 Feb – 4 Mar 2016, San Francisco, USA | 07 Sep 2015 |
| Cloud Computing | International Conference on Cloud Computing, GRIDs, and Virtualization | 20-24 Mar 2016, Rome, Italy | 3 Nov 2015 |
| EUROCRYPT | International Conference on the Theory and Applications of Cryptographic Techniques | 8-12 May 2016, Vienna, Austria | 8 Oct 2015 |
| S&P | IEEE Symposium on Security and Privacy | 23-28 May 2016, San Jose, USA | 13 Nov 2015 |
| ASIACCS | ACM Symposium on Information, Computer and Communications Security | 31 May-03 Jun 2016, Xi'an China | 20 Nov 2015 |
| PETS | Privacy Enhanced Technologies Symposium | 19-22 Jul 2016, Darmstadt, Germany | 30 Nov 2015 |

Table 1 List of relevant conferences and workshops

D7.2: Dissemination Plan

| Journal Acronym | Journal Name | Impact Factor |
| --- | --- | --- |
| TISSEC | ACM Transactions on Information and Systems Security | 1.021 |
| TDSC | IEEE Transactions on Dependable and Secure Computing | 1.351 |
| Journal of Cryptology | International Association for Cryptographic Research | 0.77 |
| TOIT | ACM Transactions on Internet Technology | 0.769 |
| TON | IEEE/ACM Transactions on Networking | 1.986 |
| TIFS | IEEE Transactions on Information Forensics and Security | 2.065 |
| S&P | IEEE Security and Privacy Magazine | 0.731 |
| C&S | Computers & Security | 1.031 |

Table 2 List of relevant journals

| Summer School Name | Dates & Location (if available) |
| --- | --- |
| IFIP Summer School on Privacy and Identity Management | 17-21 Aug 2015, Edinburgh, Scotland; expecting 2016 dates |
| COINS Summer School on Cloud Security | 22-29 Aug 2015, Methoci, Lesbos, Greece; expecting 2016 dates |
| Summer school on Secure and Trustworthy Computing | 23-27 Sep 2015, Bucharest, Romania; expecting 2016 dates |
| Summer school on elliptic curve cryptography | 23-25 Sep 2015, Bordeaux, France; expecting 2016 dates |
| Summer school on mathematical and practical aspects of fully homomorphic encryption and multi-linear maps | 12-16 Oct 2015, Paris, France |
| International School on Foundations of Security Analysis and Design | 30 Sept – 05 Oct 2015, Bertinoro, Italy |

Table 3 List of relevant summer schools

# 4   Dissemination Timeline

## 4.1   Phase 1: Community building and awareness (M1-M12)

During the first year of the projects, TREDISEC partners will first build the different target communities and initiate the dissemination of the goal of the project and the main security and privacy challenges the cloud technology is faced with.

The potential stakeholders can be reached through the active participation of TREDISEC partners to some specific events such as conferences, workshops and summer schools on the TREDISEC topics including cloud security, privacy and cryptography. TREDISEC partners will also reach different European/national/international projects which share similar topics. On the other hand, TREDISEC's industrial partners also aim at starting with engaging their internal business/product units.

The project presentation is part of the initial dissemination activities. This activity consists of producing some presentations making a general overview of the project scope and outlining the main results that should be delivered within the lifetime of the project. All TREDISEC partners will participate in these activities by describing the TREDISEC concept and approach at any event they are invited to (such as summer schools, conferences or seminars). Furthermore, a first document has already been produced and illustrated in deliverable D7.3. Another document describing the TREDISEC use cases within can also increase the awareness of mainly the business community. Some partners have already started to give presentations such as keynote speeches or even to organize workshops in order to create general awareness on TREDISEC objectives. These activities are listed in section 5.

The objectives of this first year community building and engagement activity is to also prepare people to move from awareness of the specific privacy and security challenges of the cloud environment through the understanding of the conflict between functional, non-functional and security and privacy requirements which will be mostly tackled in deliverable D2.2 "Requirements analysis and consolidation".

## 4.2   Phase 2: Dissemination of research results (M9-M36)

Once different communities are successfully built and target communities became familiar with the TREDISEC challenges, the dissemination activity will focus on the description of TREDISEC solutions. With this aim, each technical work package, namely WP3 "Verifiability with storage efficiency", WP4 "Securing Data Access in Multi-Tenant Storage Systems" and WP5 "Outsourcing and Processing Encrypted Data", will first focus on the state of the art and will prepare some report respectively on verifiability, access control and secure isolation with multi-tenancy, and, privacy preserving data processing, which will be integrated in its initial deliverable of the above mentioned WPs.

As TREDISEC partners will further propose the new TREDISEC primitives, these solutions will continuously be disseminated at each stage of their development, from their initial design until their prototyping and evaluation. The main target for such dissemination activities will be the research community and EU/national/international research projects. Project research results will be disseminated through publications and presentations in relevant scientific conferences and workshops.

TREDISEC will also organize a workshop towards the end of the project. The aim will be to gather researchers and technical experts to communicate TREDISEC results acquired during the entire lifetime of the project and therefore increase the market potential.

## 4.3   Phase 3: Dissemination of innovation results (M24-M36)

During the last year of the project, TREDISEC solutions will start to be mature enough and some of them will even be implemented. While partners will continue to publish the result of their research work, this third dissemination phase also envisions to help the task on exploitation activities by disseminating tangible results such as the demonstration of the TREDISEC tools. The TREDISEC

dissemination activity will assist people from both research and business communities in taking up TREDISEC technological results through various training workshops.

# 5 Current Dissemination Activities (M1-M9)

## 5.1 Publications

Table 4 enumerates the publications of some TREDISEC partners during M1-M9.

| Title | Authors | Conference/ journal name | TREDISEC partner(s) |
|---|---|---|---|
| **Transparent data deduplication in the cloud** | F. Armknecht, J.-M. Bohli, G. Karame, F. Youssef | ACM CCS | NEC |
| **Initial encryption of large searchable data sets using hadoop** | F. Wang, M.Kohler, A, Schaad | SACMAT | SAP |
| **PerfectDedup: Secure data deduplication** | P. Puzio, R. Molva, M. Önen, S. Loureiro | DPM | EURECOM |

Table 4 TREDISEC publications during M1-M9

## 5.2 Conference attendance, talks, project presentation, etc.

In addition, to the publications, we provide a list of relevant dissemination activities such as workshop organization or keynote speech during M1-M9 in Table 5.

| Dissemination activity | Date & Location | Event name | TREDISEC Partner |
|---|---|---|---|
| **Invited speaker** | 17-21 Aug 2015 | IFIP Summer School in Privacy and Identity Management | Melek Önen, EURECOM |
| **Workshop organization** | 30 Sep 2015 | SPC: 1st IEEE Workshop on Security and Privacy in the Cloud | Elli Androulaki, IBM |
| **Workshop organization** | 18 Sep 2015 | ZISC Workshop on Information Security | Claudio Soriente, ETHZ |
| **Seminar attendance** | 18-23 Oct 2015 | Dagstuhl Seminar on Genomic Privacy | Florian Kerschbaum, SAP |
| **Conference attendance** | 27-28 Nov 2015 | CODEMOTION | David Vallejo, ARSYS |
| **Invited speaker** | Feb 2016 | Dagstuhl Seminar on Modern Cryptography and Security: an Inter-community Dialogue | Refik Molva, EURECOM |

Table 5 List of other dissemination activities during M1-M9

# 6   Conclusions

This document has presented the main dissemination plan of the TREDISEC project. The project will approach the target dissemination communities and engage key stakeholders during the three consecutive phases, namely, "the community building and awareness" phase, "the dissemination of research results" phase and the "dissemination of innovation results" phase. The document described the target audience and a variety of appropriate dissemination channels to reach relevant stakeholders. As dissemination activities will be performed throughout the lifetime of the project, the proposed dissemination plan is subject to be changed and updated to better fit the necessities and objectives of the project.