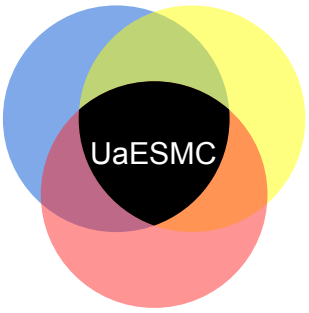

Project N°: **FP7-284731**

Project Acronym: **UaESMC**

Project Title: **Usable and Efficient Secure Multiparty Computation**

Instrument: **Specific Targeted Research Project**

Scheme: **Information & Communication Technologies**

Future and Emerging Technologies (FET-Open)

Deliverable D6.2.2
Dissemination Report

Due date of deliverable: 31st January 2014

Actual submission date: 31st January 2014

Start date of the project: **1st February 2012** Duration: **36 months**

Organisation name of lead contractor for this deliverable: **UT**

Specific Targeted Research Project supported by the 7th Framework Programme of the EC		
Dissemination level		
PU	Public	✓
PP	Restricted to other programme participants (including Commission Services)	
RE	Restricted to a group specified by the consortium (including Commission Services)	
CO	Confidential, only for members of the consortium (including Commission Services)	

Executive Summary:
Dissemination Report

This document summarizes deliverable D6.2.2 of project FP7-284731 (UaESMC), a Specific Targeted Research Project supported by the 7th Framework Programme of the EC within the FET-Open (Future and Emerging Technologies) scheme. Full information on this project, including the contents of this deliverable, is available online at `http://www.usable-security.eu`.

The second dissemination report gives an overview of UaESMC dissemination activities during the second year (M13-M24). The main objective for this period was to continue communicating the project to the target groups and to prepare for the third year dissemination activities. The dissemination activities themselves have been categorized in 3 broad groups: project web-page, conferences, seminars, presentations and workshops, and publications. The web-page has been visited approximately 832 times (598 unique visitors). The project has been presented in 6 conference/workshop talks and in 4 publications.

List of Authors

Laur Kanger (UT)

Contents

Chapter 1

Introduction

This deliverable is part of WP6 (*Dissemination*) with the main aim of introducing UaESMC to experts and wider public. For a successful communication of fairly complex SMC technologies we have identified three key target groups who need to be approached though different communication strategies:

- The first target group is the *academic circle*: on the one hand we are targeting the community of cryptographers, information security specialists or computer scientists but on the other hand, we also have additional focus on general academic public from other disciplines. The latter gives us opportunity to enhance interdisciplinary research in the areas of IT development. Dissemination activities are connected with regular research activities: publishing papers, attending conferences and sharing the knowledge project generates.

- The second target group is the *potential stakeholders* of future SMC applications (e. g., the experts in IT and security field who deal with problems that could potentially be solved with SMC). The aim of dissemination activities is getting critical feedback to the activities of the project, but also raising the awareness of the SMC solutions among the practitioners' communities. This group has a subgroup among policy makers in the related areas who can with their everyday activities influence the legal and social context in which the SMC applications would be implemented in the future.

- Thirdly the dissemination activities target the *general public* with the aim to raise general awareness of the potential of SMC in society.

This deliverable reports the dissemination of the project during the second year, giving an overview of all the dissemination activities and evaluation of second year results.

Chapter 2

Second year dissemination activities

2.1 Project website

Information pertaining to progress of the project continued to be disseminated on the website started in the first year (`http://www.usable-security.eu`). This includes references to publications and original news items (15 in 2013). Estonian section of the website was also amended with references to materials introducing the basics of SMC. In 2013 the project website was visited 832 times by 598 unique visitors. The news section continues to be updated on a regular basis.

2.2 Conferences, presentations, seminars, workshops

The following section provides an overview of UaESMC related presentations given by the project partners and presentations/seminars where UaESMC has been discussed. Only the second year activities have been included.

2.2.1 Conferences

ICA, 2013, London, UK, June 17-21, 2012

Title: Usable Security: What Do Stakeholders Expect From Secure Communication and Cooperation Technologies?
Authors: Pille Pruulmann-Vengerfeldt, Kadri Tõldsepp (UT)
Audience: Approximately 25 people

2.2.2 Presentations, seminars, workshops

Estonia Computer Science Theory Days, Otepää, Estonia, February 2, 2013

Title: Secure subset cover computation via a genetic algorithm
Authors: Jan Willemson (CYB)
Audience: 40, computer scientists

Crypto reading group at University of Tartu, Tartu, Estonia, September 5, 2013

Title: New Attacks against Transformation-Based Privacy-Preserving Linear Programmings
Authors: Alisa Pankova (CYB)
Audience: 10

Security and Trust Management 2013 (workshop), Royal Holloway, Egham, UK, September 12-13, 2013

Title: New Attacks against Transformation-Based Privacy-Preserving Linear Programmings
Authors: Peeter Laud, Alisa Pankova (CYB)
Audience: 30

Nutipäev 2013, Tartu, Estonia, November 16, 2013

Title: Mida peaks teadma inimeste sotsiaalkäitumisest enne nutiturvalahenduste projekteerimist
Authors: Pille Pruulmann-Vengerfeldt (UT)
Audience: Approximately 60 IT practitioners and military enthusiasts

Developments and Challenges in Business Surveys Methodology (A seminar organised by ENBES and the Swedish Survey Methodology Association), Stockholm, Sweden, January 21, 2014

Title: Enhanced security guarantees for sensitive statistical studies
Authors: Baldur Kubo (CYB)
Audience: 50 statisticians from 8 countries

2.2.3 Publications

Talviste Riivo; Laur, Sven; Willemson, Jan. **From Oblivious AES to Efficient and Secure Database Join in the Multiparty Setting.** *The 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)*, June 2013. Published.

Laud, Peeter; Pankova, Alisa. **New Attacks against Transformation-Based Privacy-Preserving Linear Programming.** *Security and Trust Management STM 2013*, December 2013. Published.

Laud, Peeter; Pankova, Alisa. **On the (Im)possibility of Privately Outsourcing Linear Programming.** *The ACM Cloud Computing Security Workshop (CCSW 2013)*, November 2013. To appear.

Kiayias, Aggelos; Tselekounis, Yiannis. **Tamper Resilient Circuits: The Adversary at the Gates.** *ASIACRYPT 2013*, December 2013. To appear.

Chapter 3

Evolution of the results and future activities

During the first year the targeted groups were communicated by the website, direct contacts, deliverables, conferences, seminars and workshops. These types of activities were continued during the second year. In order to target the academic circle more efficiently academic papers were employed as an additional medium of communication. Four papers were prepared by the project participants in 2013 (two already published, two to appear).

In the third year there will be a renewed stress on direct contacts. Prototype applications using SMC techniques will be used in conducting additional interviews with members of the academic circle and potential stakeholders. Leaflet, a slide show and a cartoon demonstrating selected SMC applications will be used as introductory materials in order to facilitate the interviews and lower the learning barrier. These materials will also be shared on the web and possibly used in seminars.

The feedback from the interviewees will be used to finalize the project. The end results will be disseminated to various audiences especially taking into account the trans-disciplinary aspect of the project (innovation as well as the communication of innovation). Together with this report there will be 8 new deliverables published in the end of M24, creating an excellent basis for the third year dissemination work. At the moment the project participants are already actively searching for dissemination opportunities. The main strategies include:

- participation in conferences and the organization of panels in particular, e.g. in the 2015 Computers, Privacy and Data Protection conference
- organization of workshops targeted towards academics and research-oriented experts on one hand, and security experts and potential users of SMC applications on the other
- seeking for opportunities to publish a book based on project outcomes, e.g. with IOS Press which has previously published material on secure multi-party computation.