This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 609611.

D32.2

Intermediate report on dissemination, standardisation, exploitation and training

Project number:	609611
Project acronym:	PRACTICE
Project title:	PRACTICE: Privacy-Preserving Computation in the Cloud
Start date of the project:	1st November, 2013
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	ICT-609611 / D32.2 / 1.0
Activity and Work package contributing to the deliverable:	Activity 3 / WP32
Due date:	October 2015 – M24
Actual submission date:	3rd November, 2015

Responsible organisation:	UMIL
Editor:	Stelvio Cimato
Dissemination level:	Public
Revision:	1.0

Abstract:	This deliverable reports on the progress and further plans of the project partner for their dissemination activities, standardisation and exploitation of project results, and project internal/external education and training.
Keywords:	Dissemination, Training, Standardisation, Exploitation

Editor

Stelvio Cimato (UMIL),

Marion Buchacher (TEC)

Contributors (ordered according to beneficiary numbers)

TEC	Technikon Forschungs- und Planungsgesellschaft mbH, Austria
SAP	SAP AG, Germany
TUDA	Technische Universität Darmstadt, Germany
ALX	Alexandra Instituttet A/S, Denmark
ARC	Arçelik A.Ş., Turkey
BIU	Bar Ilan University, Israel
CYBER	Cybernetica AS, Estonia
UWUERZ	Julius-Maximilians Universität Würzburg, Germany
INTEL	Intel GmbH, Germany
KU Leuven	Katholieke Universiteit Leuven, Belgium
INESC PORTO	Inesc Porto – Instituto de Engenharia de Sistemas e Computadores do Porto, Portugal
AU	Aarhus Universitet, Denmark
TUE	Technische Universiteit Eindhoven, Netherlands
UNIVBRIS	University of Bristol, United Kingdom
DTA	Distretto tecnologico aerospaziale S.c.a.r.l., Italy
UMIL	Universita degli studi di Milano, Italy
PAR	Partisia APS, Denmark
UGOE	Georg-August-Universität Göttingen Stiftung öffentlichen Rechts, Germany

Disclaimer

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609611 (PRACTICE).

Executive Summary

This deliverable reports on the activities of the project partners in terms of dissemination of the project, standardisation and exploitation of project results, and project internal/external training during the second year of the PRACTICE project.

The consortium is composed of strong academic and industrial partners, involved at different roles in the organization of scientific and industrial events. The impact of the project in the international scientific community working in related themes, such as cloud computing and cryptography, is proved by a discrete number of publications included in the most important journals, as well as in the most important conferences of the area. Moreover, industrial partners have participated/organized a large number of events aiming to attract interested people and raise the public awareness of the project results.

Furthermore, this deliverable reports on internal and external training activities, including summer/winter schools open to the participation of people not directly involved in the project, and on the exploitation activities undertaken by the project partners. In particular some successful experiences are included, as well as some benefits which the partners collected within the participation in the consortium.

As usual, the dissemination activities are supported by the deployment of common dissemination channels, such as the project website, a blog, Twitter account, the participation to social networks, which have been extensively used to further extend the knowledge about the project's activities in both scientific and professional communities.

To summarize the achievements and work towards the project goals of the second project year for dissemination and standardisation we include: 26 peer-reviewed scientific publications, 35 presentations in conferences or organized events (workshops, winter/summer schools) with an international audience and very good feedback, contributions to privacy and cloud technology standards in international standardisation bodies.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose subject to any liability which is mandatory due to applicable law. The users use the information at their sole risk and liability.

Contents

List of Figures

List of Tables

Chapter 1 Dissemination

The dissemination strategy aims to ensure visibility and awareness of the project results, which have been depicted in D32.1. Some indicators have also been selected in order to return a measure of the achieved goals and evaluate how effective the dissemination activities have been executed during the time to create public interest in the project and promote its results to the interested parties. This document reports on all the dissemination activities already executed during the second year and discusses the achieved targets after monitoring of the activities, and the corrective actions if needed, to change and adapt the overall plan.

1.1 Overall dissemination strategy and evaluation criteria

As already explained in D32.1, the PRACTICE dissemination strategy adopted for the entire project duration relies on the following pillars:

- Presentation of the research results within the scientific community (section 1.2.1),
- Presentation and demonstration at national and international exhibitions & fairs and dedicated road-show events and industrial days (section 1.2.2).
- Presentation of the project to the general public (press, web, etc.) (section 1.2.3)
  - Project website (section 1.2.3.1)
  - Regular communication with the press (e.g. press releases at beginning of project, before main fairs/exhibitions)
  - Posters, handouts, and templates are provided to all partners
- Social media (section 1.2.4)
- Cooperation with other projects (section 1.2.4.2)

In the initial dissemination plan the audience has been classified into three broad categories:

- Scientific communities,
- Commercial and industry experts,
- General public.

With respect to these classification, the dissemination strategy had selected scientific publications and presence in academic events or conferences to target the scientific community, participation to events and other related outreach activities in order to interact with the eventual beneficiaries of the PRACTICE technology, and the website and other communication means such as blogs, social networks (Twitter, LinkedIn, etc.) newsletters, and produce dissemination materials easily accessible from different channels, to reach the general public.

In order to measure the progress towards fixed goals of the dissemination activities a number of KPI (Key Performance Indicator) has been selected, and periodically monitored, so that errors in the dissemination plan can be easily detected and appropriate countermeasures undertaken, eventually. Once the KPI are measured, every activity is evaluated in order to assess if both the dissemination plan is achieving the fixed goals and if the indicators themselves are appropriate for the measurement. The selected KPIs are listed in Table 1, while a detailed discussion of each dissemination activity and the associated KPIs is reported in each section.

Dissemination activity/channel	KPI	Target values
Website	• Number of visits • Number of unique visitors	• ≥3650 • ≥1825
Scientific Conferences and Journals	• Number of publications per year • Number of attendees • Impact factor • Feedback received • Number of citations	• ≥11 • ≥330 • ≥ 2 top 20 • -- • ≥10
Newsletters/Fact Sheets/Posters	• Number of contacts • Number of downloads	• ≥50 • ≥100
Social Networks/Blogs	• Number of contacts • Number of posts/messages	• ≥50 • ≥24
Presentation/Workshops	• Number of attendees • Number of events	• ≥300 • ≥10

Table 1: Key performance indicators for the dissemination activities

1.2 Dissemination activities started in M13-M24

The project and its results have been disseminated by invited talks at conferences, by publications at scientific and industry oriented conferences (such as ACM CCS, CSP Forum, ASIACCS, NDSS Symposium, etc.) 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.

1.2.1 Scientific publications

The following scientific peer-reviewed publications have been published within the second PRACTICE project year. All scientific publications are listed in an action overview list and are updated by the partners on a regular basis. Currently *26 peer-reviewed scientific publications* were prepared during the second project year. Altogether *48 publications* have been created since project start (M01-M24).

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publication?
How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation (Short Paper)	Dan Bogdanov, Marko Jõemets, Sander Siim, Meril Vaht	Financial Crypto 2015	Financial Crypto	Puerto Rico	2015	Multiple times shared publication with public sector organization. Created international interest against the solution.	Request to estimate cloud cost & feasibility received and processed within PRACTICE.	NA	http://practice-project.eu/downloads/publications/How-Estonian-Tax-Customs-Board-Evaluated-Tax-Fraud-Detection.pdf	Yes
ABY - a framework for efficient mixed-protocol secure two-	Daniel Demmler, Thomas Schneider, Michael	Network and Distributed System Security Symposium	The Internet Society	San Diego (CA)	2015	The framework has already been used in other publications.	Accepted at the 6th top conference in security and privacy, with	8 (from February to October 2015)	http://encrypto.de/papers/DSZ15.pdf	Yes

[1] References to conference ratings are according to the Microsoft academic research ranking of top conferences in security and privacy with field rating: http://academic.research.microsoft.com/RankList?entitytype=3&topdomainid=2&subdomainid=2.

[2] 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).

[3] 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	Place of publication	Year of publica-tion	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publi-cation?
party computation	Zohner	(NDSS)					acceptance rate 18.4%.			
An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-Programmable Random Oracle	Yehuda Lindell	Theory of Cryptography Conference (TCC)	TCC	Warsaw (Poland)	2015	NA	NA	NA	http://practice-project.eu/downloads/publications/sigma-to-nizk.pdf	Yes
Adaptive Proofs of Knowledge in the Random Oracle Model	David Bernhard, Marc Fischlin, Bogdan Warinschi	PKC	Springer	Washington DC (USA)	2015	NA	Accepted at one of the workshops of the IACR	4 (since April 2015)	NA	Yes
Additively Homomorphic UC Commitments with Optimal Amortized Overhead	Ignacio Cascudo, Ivan Damgård, Bernardo Machado David, Irene Giacomelli, Jesper Buus Nielsen, Roberto Trifiletti	PKC	Springer	Washington DC (USA)	2015	Used in follow up work.	Accepted at one of the workshops of the IACR	4 (since April 2015)	http://practice-project.eu/downloads/publications/Additively-Homomorphic-UC-Commitments.pdf	Yes
Oblivious Outsourcing of Garbled Circuit Generation	Florian Kerschbaum	ACM SAC	ACM	Salamanca	2015	NA	NA	NA	http://dx.doi.org/10.1145/2695664.2695665	Yes
More efficient oblivious	Gilad Asharov, Yehuda	Eurocrypt 2015	Springer	Sofia	2015	Collaboration between	Accepted at the 2nd top	6 (from April to	http://eprint.iacr.org/2015	No

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publication?
transfer extensions with security for malicious adversaries	Lindell, Thomas Schneider, Michael Zohner					partners TUDA and BIU.	conference in security and privacy, with acceptance rate 29.4%.	October 2015)	/061	
Ciphers for MPC and FHE	Martin Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, Michael Zohner	Eurocrypt 2015	Springer	Sofia	2015	The paper implied further research on block cipher design.	Accepted at the 2nd top conference in security and privacy, with acceptance rate 29.4%.	9 (from April to October 2015)	http://dx.doi.org/10.1007/978-3-662-46800-5_17	No
Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge	Tore Kasper Frederiksen, Jesper Buus Nielsen, Claudio Orlandi:	Eurocrypt 2015	Springer	Sofia	2015	Generated follow up work	Accepted at one the flagship conferences of the IACR	4 (since May 2015)	http://dx.doi.org/10.1007/978-3-662-46803-6_7	No
TinyGarble: Highly compressed and scalable sequential garbled circuits	Ebrahim M. Songhori, Siam U. Hussain, Ahmad-Reza Sadeghi, Thomas Schneider, Farinaz Koushanfar	S&P'15: 36th IEEE Symposium on Security and Privacy	IEEE	San Jose (CA)	2015	The paper introduced a new approach used in later publications.	Accepted at the 3rd top conference in security and privacy, with acceptance rate 13.5%.	5 (from May to October 2015)	http://practice-project.eu/downloads/publications/TinyGarble-Highly-Compressed-Scalable-Sequential-Garbled-Circuits.pdf	Yes
ADSNARK: Nearly-	M. Backes, M. Barbosa, D.	S&P'15: 36th IEEE	IEEE	San Jose (CA)	2015	An extension to the open	Accepted at the 3rd top	13 from May to October	https://eprint.iacr.org/2014	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publication?
Practical Privacy-Preserving Proofs on Authenticated Data.	Fiore, R. M. Reischuk	Symposium on Security and Privacy				source cryptographic library libsnark.	conference in security and privacy, with acceptance rate 13.5%.	2015	/617.pdf	
Possibilistic assessment of process-related disclosure risks on the cloud	Ernesto Damiani, Valerio Bellandi, Stelvio Cimato, and Gabriele Gianini	In "Computational Intelligence and Quantitative Software Engineering"	Springer		2015	Book chapter	NA	NA	NA	No
Universally Verifiable Multiparty Computation from Threshold Homomorphic Cryptosystems	Berry Schoenmakers, Meilof Veeningen	ACNS	Springer	New York (USA)	2015	International conference	Accepted at ACNS 2015	1	http://eprint.iacr.org/2015/058	Yes
Policy Privacy in Cryptographic Access Control	A.L. Ferrara, G. Fachsbauer, , Bin Liu, B. Warinschi	CSF	ACM		2015	NA	Accepted at a top security conference	NA	http://dx.doi.org/10.1109/CSF.2015.11	Yes
Phasing: Private set intersection using permutation-based hashing	Benny Pinkas, Thomas Schneider, Gil Segev, Michael Zohner	USENIX Security Symposium 2015	USENIX	Washington DC	2015	Collaboration between partners TUDA and BIU.	Accepted at the 5th top conference in security and privacy, with acceptance	1 (from August to October 2015)	http://eprint.iacr.org/2015/634	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publica-tion	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publi-cation?
							rate 15.7%.			
Efficient Constant Round Multi-Party Computation Combining BMR and SPDZ	B. Pinkas, Y. Lindell, N. P. Smart, A. Yanai	CRYPTO 2015	CRYPTO 2015	Santa Barbara (USA)	2015	The first secure PSI protocol.	NA	NA	http://practice-project.eu/downloads/publications/mpc-BMR-SPDZ.pdf	Yes
The Simplest Protocol for Oblivious Transfer	Tung Chou, Claudio Orlandi	LATINCRYPT	Springer	Guadalajara (Mexico)	2015	No impact yet	Accepted at an event organized in cooperation with IACR	0 (presented in August 2015)	http://dx.doi.org/10.1007/978-3-319-22174-8_3	No
Time to rethink: Trust brokerage using trusted execution environments	Patrick Koeberl, Vinay Phegade, Anand Rajan, Thomas Schneider, Steffen Schulz, Maria Zhdanova	TRUST 2015	Springer	Heraklion	2015	Collaboration between partners TUDA and INTEL.	Accepted at the TRUST conference with acceptance rate 35.7%.	No citations yet (from August to October 2015)	http://dx.doi.org/10.1007/978-3-319-22846-4_11	No
Automated synthesis of optimized circuits for secure computation	Daniel Demmler, Ghada Dessouky, Farinaz Koushanfar, Ahmad-Reza Sadeghi, Thomas Schneider, Shaza Zeitouni	ACM Conference on Computer and Communications Security (CCS)	ACM	Denver	2015	No impact yet (presented in October 2015).	Accepted at the 4th top conference in security and privacy, with acceptance rate 19.8%.	No citations yet (presented in October 2015)	http://dx.doi.org/10.1145/2810103.2813678	No
The Analysis	Meril Vaht	Master's thesis	-	Tartu	2015	A real-world	NA	NA	https://share	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publica-tion	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publi-cation?
and Design of a Privacy-Preserving Survey System		of the University of Tartu				survey system is built according to the design.			mind.cyber.ee/files/papers/privacy_preserving_survey_system_vaht_2015.pdf	
Frequency-Hiding Order-Preserving Encryption	Florian Kerschbaum	ACM Conference on Computer and Communications Security (CCS)	ACM	Denver	2015	NA	NA	NA	http://dx.doi.org/10.1145/2810103.2813629	Yes
SEDA: Scalable Device Attestation	N. Asokan, Ferdinand Brasser, Ahmad Ibrahim, Ahmad-Reza Sadeghi, Matthias Schunter, Gene Tsudik, Christian Wachsmann	ACM Conference on Computer and Communications Security (CCS), 2015	ACM		2015	No impact yet (presented in October 2015).	Accepted at the 4th top conference in security and privacy, with acceptance rate 19.8%.	No citations yet (presented in October 2015)	http://dx.doi.org/10.1145/2810103.2813670	No
Fast Garbling of Circuits Under Standard Assumptions	S. Gueron, Y. Lindell, A. Nof, B. Pinkas	ACM Conference on Computer and Communications Security (CCS)	ACM	Denver	2015	Provide new methods for garbling that are secure.	NA	NA	http://practice-project.eu/downloads/publications/fastgarbling_standard_assumptions.pdf	Yes
Secure Deduplication of Encrypted	J.Lui, N. Asokan, B.	ACM Conference on Computer and	ACM	Denver	2015	NA	NA	NA	http://eprint.iacr.org/2015	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publica-tion	Impact of publication	Feedback received[1]	Number of citations	Permanent identifiers[2] (if available)	Is/Will open access[3] provided to this publi-cation?
Data without Additional Independent Servers	Pinkas	Communications Security (CCS)							/455.pdf	
Universally Verifiable Outsourcing and Application to Linear Programming	Sebastiaan de Hoogh, Berry Schoenmakers, Meilof Veeningen	Applications of Secure Multiparty Computation (Book)	IOS Press	Amsterdam	2015	Book chapter, invited	Accepted	NA	http://dx.doi.org/10.3233/978-1-61499-532-6-186	Yes
Towards Economics Aware Risk Assessment on the Cloud	V. Bellandi, S. Cimato, E. Damiani, G. Gianini, A. Zilli	IEEE Security & Privacy	IEEE		2015	NA	NA	NA	NA	No

Table 2: List of publications

1.2.1.1 Analysis of the publications

The 26 publications reported in Table 2 give evidence of the scientific production of the consortium members, who have disseminated the projects' results in conferences and workshops, journals, books and other publications.

The KPIs, that have been selected, have the goal to check both the quantity and the quality of the dissemination activities performed by the partners during the time the project is active.

As regards the quantity, KPI "**Number of publications per year**" should measure how many scientific publications have been produced during the project and published in proceedings of conferences and workshop, or in international journals. A reasonable threshold value for the KPI seems to be 11, considering that the consortium is composed of 18 members, of which (more than) a half are academic partners (precisely 11). The target value amounts to have an average of one publication for each academic partner per year. This threshold has been overcome easily in both project years as more than 20 papers have been published per year.

The other KPIs are related to the quality of the dissemination activities resulting for the scientific publications, aiming to report on the overall impact of the work in the scientific community. We discuss here some threshold values that have been selected for each KPI. For the "**Number of attendees**", a value ≥ 330 seems to be acceptable, since it means that for each of the foreseen 11 publications, at least 30 attendees per event have been contacted (see Table 3). At the moment most of the publications have targeted the most important scientific events, collecting hundreds of persons each.

Traditionally, the Impact Factor (IF) is related to journals and returns the average number of times articles from the journal published in the past two years have been cited in the Journal Citation Reports year. The IF is commonly accepted, even with some founded criticisms, as a measure reflecting the relative importance of a journal within its field, where higher impact factors denote journals more important than those with lower values. Since most of the publications are included in conferences, we adapted the KPI to take into account the impact of conferences. To this aim we considered different rankings, since no "official" ranking has been determined by any international institution or authority, but online a number of rankings are available based on different criteria, ranging from considering the Conference Impact factor, to the h-index, or the impact factor associated with the published proceedings of the conference. We considered the following rankings:

- Google scholar ranking (based on the h5-index is the h-index for articles published in the last 5 complete years),

  https://scholar.google.com/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography

- Microsoft academic research

  http://academic.research.microsoft.com/RankList?entitytype=3&topdomainid=2&subdomainid=2&last=0&orderby=6

- Top Crypto and Security Conferences Ranking held by Jianying Zhou. (based on the Conference Impact Factor (CIF): http://icsd.i2r.a-star.edu.sg/staff/jianying/conference-ranking.html

- Computer Security Conference Ranking and Statistic by Guofei Gu http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm

The threshold for the KPI regarding "**Impact factor**" for conferences has been turned in having at least 2 papers (out of 11 foreseen publications) in the top 20 conferences. This KPI has been overcome by a large amount, having 10 papers published in the top 10 conferences in 2015.

As regards the "**Number of citations**", the KPI should determine the impact of the scientific production counting how many citations the papers published have been received. Since citations grow with time passing, we set a threshold value at 11, meaning that of the 11 foreseen publications, on average they should have been cited at least 1 time. Also this KPI has been satisfied, and many papers have been cited multiple times in this year to testify the deep impact they had in the related field on the community of researchers.

Finally, we decided to not consider the KPI related to the received feedback, since it was difficult to measure taking account some established metric. Looking at Table 2, some notes aim to register the interest papers have received when they were presented.

Concluding Remark: The dissemination activities performed during the second year, satisfy the KPIs achieving successful results both for quality and quantity of the scientific publications. The great number of actions are accompanied with the selection of the most important conferences in the area targeting the most active researchers and involving a large number of people interested into the project topics.

1.2.2 Presentations, conferences and workshops

All Presentations, Conferences and Workshops are listed in an action overview list and are updated by the partners on a regular basis. Currently the PRACTICE partners participated in 35 events including presentations, conferences and workshops during the second project year. In this period, the dissemination towards commercial audience and industry experts has been increased, with the participation to a large number of exhibitions and fairs, to attract the attention of people interested in the exploitation of the project results. In the following table, all the activities are listed, reporting the type of activity and the dissemination target, and all the details about the event.

Type of activities/ Dissemination target	Main leader	Title	Date			Place	Size of audience	Impact, type and goal of the event	Countries addressed
			Day	Month	Year				
Conference	TEC	Connect 2014	13	11	2014	Klagenfurt, Austria	-	PRACTICE was presented to interested audience.	National
Workshop	INTEL	W3C Workshop on User-Centric Privacy Controls	20	11	2014	Berlin, Germany	40	Workshop on standardisation of Internet privacy controls by W3C; The workshop was chaired by M. Schunter (Intel)	International
Other	ARC	NESSI Members and International Cooperation Days	20-21	11	2014	Barcelona, Spain	120	PRACTICE brochures were distributed	International
Exhibition	ARC	Turkey Innovation Week	4-6	12	2014	Istanbul, Turkey	~40,000	Arcelik was the main sponsor of this event and has presented PRACTICE project at its booth in the exhibition area	National
Working Group	TUE	Cryptography Working Group	5	12	2014	Utrecht, The Netherlands	40	Update Dutch cryptographers on secure computation and PRACTICE	National
Workshop	CYBER	Real World Crypto Workshop 2015	7-9	1	2015	London, UK	400	We demonstrated PRACTICE technologies at the Real World Crypto 2015 conference.	International
Conference	TUDA	NDSS Symposium	8-11	1	2015	San Diego, USA	-	TUDA presented PRACTICE at the Symposium	International
Conference	TUDA	AAAS Annual Meeting	12-16	1	2015	San Jose, USA	8.000	TUDA presented PRACTICE at the Symposium	International
Other	ARC	Big Data networking days	16	1	2015	Brussels, Belgium	~200	PRACTICE Brochures distributed and info given to the interested parties during the H2020 ICT-16 Big Data networking day in Brussels	International
Workshop	SAP	Financial Cryptography 2015	26-30	1	2015	Puerto Rico, USA	50	We prepared a competition task for the secure genome analysis competition and participated to present it. It turned out that the competition was not aware of some of the technologies used in	International

Type of activities/ Dissemination target	Main leader	Title	Date			Place	Size of audience	Impact, type and goal of the event	Countries addressed
			Day	Month	Year				
								PRACTICE and we ended up being disadvantaged in the competition. In one task (secure genome comparison in the multi-party setting), we had the fastest solution, but were disqualified due to the organizers deciding that the third server used too much (2 CPU cores) resources. They were also unsure of the legal status of three-party multi-party computation. By attending, we were able to show the benefits of PRACTICE statistics work and also explain our legal analysis. The interest to the PRACTICE legal work was especially strong. The organizers promised to modify the competition rules for the next year so more of our efficient technologies could be acceptable.	
Exhibition	DTA	Engineering knowledge management for product lifecycle optimization, trends, approaches and new insights	5-6	2	2015	Italy	-	Participation with an information stand at the workshop	International
Other	BIU	5th BIU winter school	15-19	2	2015	Ramat Gan, Israel	100	In the setting of secure multiparty computation, two or more parties with private inputs wish to compute some joint function of their inputs. The security requirements of such a computation are privacy (meaning that the parties learn the output and nothing more), correctness (meaning that the output is correctly distributed), independence of inputs, and more. This setting encompasses computations as simple as coin-tossing and agreement, and as complex as electronic voting, electronic auctions, electronic cash schemes, anonymous transactions, and private information retrieval schemes. Due to its generality, secure computation is a central tool in cryptography.	International
Conference	ARC	H2020 Industry Working Day -	20	2	2015	Ankara, Turkey	~500	PRACTICE brochures were distributed during the German-Turkish Year of Research Closing	Europe

Type of activities/ Dissemination target	Main leader	Title	Date			Place	Size of audience	Impact, type and goal of the event	Countries addressed
			Day	Month	Year				
		TUBITAK						Ceremony	
Conference	ARC	German-Turkish Year of Research Closing Ceremony	12	3	2015	Ankara, Turkey	~700	PRACTICE brochures were distributed at Arcelik stand during the event.	International
Workshop	CYBER	Secure Genome Analysis Competition at the IDASH Privacy and Security Workshop 2015	16	3	2015	San Diego, CA, USA	30	We published a paper at Financial Cryptography 2015 and presented it.	International
Conference	ARC	Turkey Innovation Week	19-20	3	2015	Izmir, Turkey	30.000	PRACTICE brochures were distributed during Net Futures 2015	Europe
Conference	ARC	Net Futures 2015	25-26	3	2015	Brussels, Belgium	700	PRACTICE was presented to interested audience.	Europe
Conference	TUDA	10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)	14-17	4	2015	Singapore, Asia	182	TUDA presents PRACTICE at the Symposium	International
Conference	SAP	ACM SAC	16-17	4	2015	Salamanca, Spain	-	We published a paper at Financial Cryptography 2015 and presented it.	International
Conference	TEC	CSP Forum	28-29	4	2015	Brussels, Belgium	500	PRACTICE was presented to interested audience.	International
Conference	AU	EUROCRYPT 2015	26-30	4	2015	Sofia, Bulgaria	400	AU presented one PRACTICE paper in the conference	International
Workshop	INESC PORTO	COST CRYPTOAction [http://cryptoaction.eu/wgmeeting-ec2015.html]	26	4	2015	Sofia, Bulgaria	-	Organised a working group meeting in the area of quasi-practical cryptographic solutions for the cloud, where the work carried out in PRACTICE was discussed.	International
Conference	ARC	Turkish Industry in Horizon 2020 Forum	6	5	2015	Ankara, Turkey	over 600	PRACTICE project was mentioned in the success story presentation of Arcelik and PRACTICE brochures were distributed to the participants.	International

Type of activities/ Dissemination target	Main leader	Title	Date			Place	Size of audience	Impact, type and goal of the event	Countries addressed
			Day	Month	Year				
Conference	TUE	ACNS 2015	2-5	6	2015	New York, USA	100	Presented paper on verifiable secure computation	International
Workshop	BIU, AU	Workshop on secure multiparty computation	8-12	6	2015	Berkeley, USA	-	The workshop is very related to the research which is performed in PRACTICE. Thus, BIU and AU will participate to learn more about the topic	International
Conference	TUDA, INTEL	TRUST2015	22-27	8	2015	Heraklion, Greece	-	Chairing and presentation by M. Schunter (Intel)	International
Conference	AU, TU/e	LATINCRYPT 2015	23-26	8	2015	Guadalajara, Mexico	150	One PRACTICE paper was presented.	International
Conference	ARC	OpenLivingLab Days 2015	25-28	8	2015	Istanbul, Turkey	170	OpenLivingLab Days is the annual summit of the worldwide Living Lab community integrated with the popular ENoLL Summer School. The annual 4 day event includes interactive sessions, workshops, lively discussion panels with excursions and off-site visits with the aim of giving the participants a wider insight about models, theories and technologies related to Living Labs.	International
Workshop	All partners	PRACTICE Summer School	23-27	9	2015	Bucharest, Romania	~ 70	PRACTICE in collaboration with the Polytechnic Institute Bucharest organizes a summer school on topics related to Secure and Trustworthy Computing	International
Workshop	ARC	Horizon 2020 Workshop	5-6	10	2015	Bursa, Turkey	~200	PRACTICE project was mentioned in the success story presentation of Arcelik and PRACTICE brochures were distributed to the participants.	National
Conference	ARC	Conference on Turkish Universities in the European Research Area (ERA)	8-9	10	2015	Ankara, Turkey	~500	Arçelik was the main sponsor of the event and PRACTICE project poster were shown at Arcelik stand in the exhibition area and PRACTICE brochures were distributed to the participants.	Europe
Conference/Workshop	ARC	Horizon 2020 Bridging Days	12-13	10	2015	Izmir, Turkey	~250	PRACTICE project was mentioned in the success story presentation of Arcelik and PRACTICE brochures were distributed to the participants.	Europe
Conference	TUDA, BIU	22nd ACM Conference on	12-16	10	2015	Denver, USA	-	TUDA and BIU presents PRACTICE at the conference	International

Type of activities/ Dissemination target	Main leader	Title	Date			Place	Size of audience	Impact, type and goal of the event	Countries addressed
			Day	Month	Year				
		Computer and Communications Security							
Exhibition	DTA	Supply Chain Management optimization: security issues and business risks	14-15	10	2015	Paris, France	-	Presentation of DTA activities and results achieved through PRACTICE project. Distribution of leaflet and info to aerospace industry representatives	International
Conference	ARC	ICT Event 2015	20-22	10	2015	Lisbon, Portugal	>5000	The biggest Information and Communication Technologies event (ICT) in Europe. The ICT 2015 event had a number of parallel activities: A policy conference presenting the new Commission's policies and initiatives on Research & Innovation in ICT (Horizon 2020 Programme); An interactive exhibition showcasing the results and impact of the most recent EU ICT Research & Innovation projects; Many networking opportunities to enhance quality partnerships, helping participants find partners, connect Research and Innovation and trigger collaboration; Funding opportunities: ICT 2015 will also be the place to gather information on the 2016-17 Work Programme of Horizon 2020.	International
Conference	CYBER	Regular meeting of ISO/IEC JTC1 SC27	26-30	10	2015	Jaipur, India	-	Representing the PRACTICE contributions to privacy standards (SP Privacy Engineering Framework, NWIP Privacy-enhancing data de-identification, 19592-1/2)	National

Table 3: Presentations, conferences and workshops

1.2.2.1 Analysis of presentations, conferences and workshops

As included in the dissemination strategy presented in D32.1, the commercial dissemination activities have been increased, and the partners have organized presentations involving a large number of attendees.

Since almost half of the consortium members are commercial partners (7 out of 18), we set as threshold values for the KPIs related to "**Number of events**" 10, and set "**Number of attendees**" to 1000, intending to target on average 100 persons per each of the foreseen 10 events.

Also in this case, the thresholds have been abundantly overcome, since most of the events attracted hundreds of persons. It is also important to register that the geographic location of the events also include countries outside of Europe, extending the dissemination of the project's results.

1.2.3 Presentation of the Project to the general public

The dissemination activities to present the project's results to the general public rely on the diffusion of news on the website, the usage of social media, newsletters, and other publications targeted at potentially interested people.

1.2.3.1 PRACTICE project website

The project website, launched in month two of the project, is available at http://www.practice-project.eu. The website has been one of the most important dissemination channels, providing continuously updated information on the project, its activities and results. The website provides all the important related information, such as contact details, partners and events, as well.

Being based on the Content Management System (CMS) "Joomla!", the website has been flexible enough to act as information center for all kind of audience and as a repository that can be accessed only by members.

The project website has been managed and maintained by the Project Coordinator, who updated the info and collected all the important news and developments provided by the partners.

Besides the structure explained in D32.1 an extra section on the "Expected impact and Progress" was added under the link About and will be updated after each project period. Furthermore, an additional link called Project Results was added which is divided in four sub items:

- Publications (publications provided by the PRACTICE consortium)
- Deliverables (public and approved deliverables)
- Application Scenarios (short videos visualizing the basic idea behind the application scenarios)
- Toolbox (links to the PRACTICE Secure Survey Platform and the Sharemind platform)

A new sub item called "Cooperation Activities" was added to the main menu of the project website called "Links" where the cooperation activities with external organisations and other projects and programmes are described.

1.2.3.2 Report on the usage of the website

A statistical analysis of access (both unique visitors and overall visits) to the PRACTICE project website (graphical visualisation) has been created which can be found below. In order to obtain these figures, we used two different statistical tools (Google Analytics and AWStats).

The following figures give attention to the second project period from the 1st of November 2014 to the end of October 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.

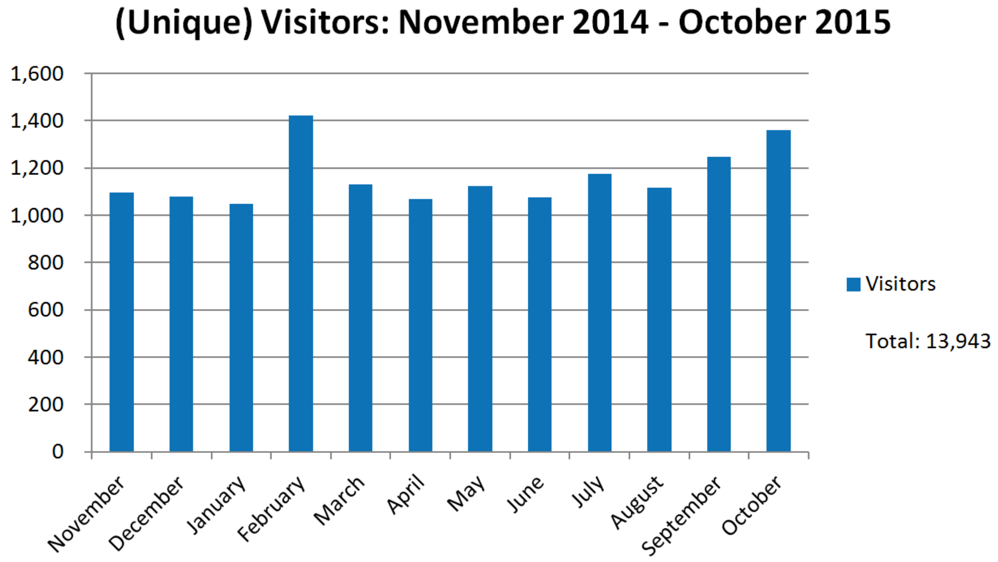


Figure 1: PRACTICE website statistic of unique visitors

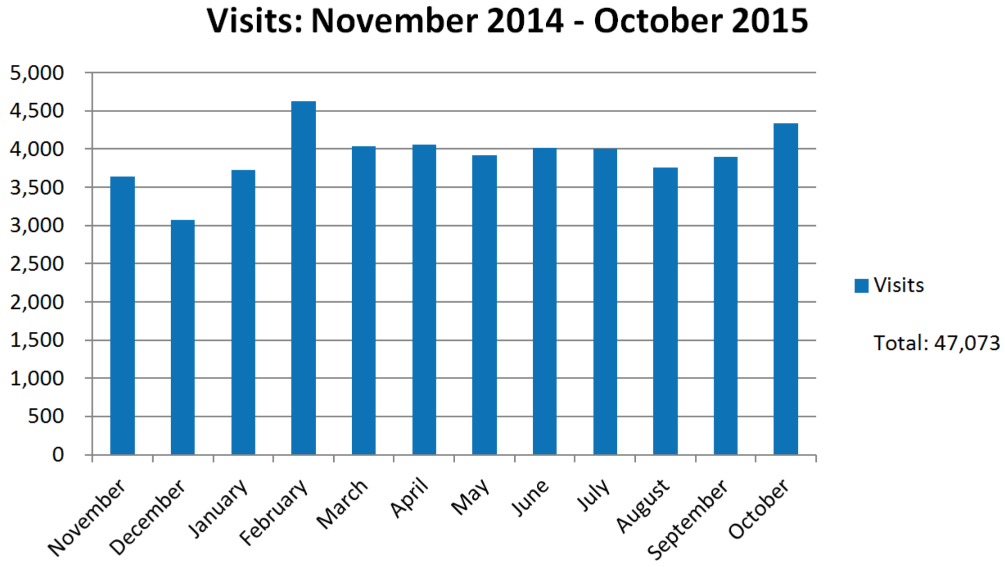


Figure 2: PRACTICE website statistic of non-unique visits

During the second project period the PRACTICE website has been visited 47,073 times in total by 13,943 unique visitors. These numbers reflect the growing popularity of the PRACTICE project. In year one the website was visited 5,679 times by 2,548 visitors.

The following website statistic (Figure 3) illustrates the geographical distribution of the visitor's location. More than a half of the visitors were from the Europe and almost one third is represented by America (Northern and South America and the Caribbean). The remaining percentage is spread over Asia, Africa and Oceania (Australia, New Zealand and New

Guinea). This shows that during the past project period the major interest in this European research project lies of course within the Europe, but it must be also highlighted that the project raises considerable interest in America. This might be due to the presentation of PRACTICE at conferences in the US, such as NDSS Symposium, AAAS Annual Meeting, ACNS 2015 or ACM CCS and some corresponding workshops.

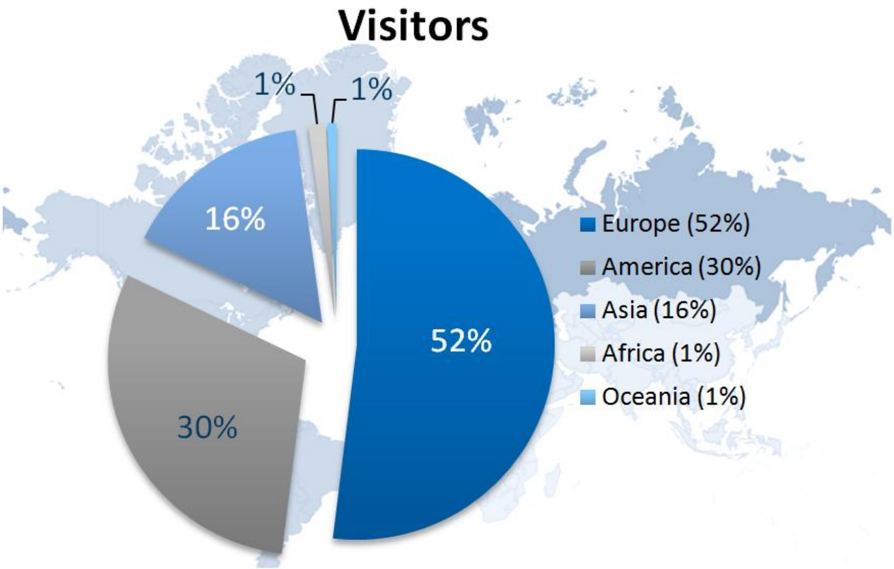


Figure 3: PRACTICE website statistic of the geographical distribution of visitor's location

With respect to the following statistic (Figure 4), it has to be pointed out that in the second project period of PRACTICE, the website has been able to attract a considerable amount of new visitors, representing more than 80% of the overall visitors.

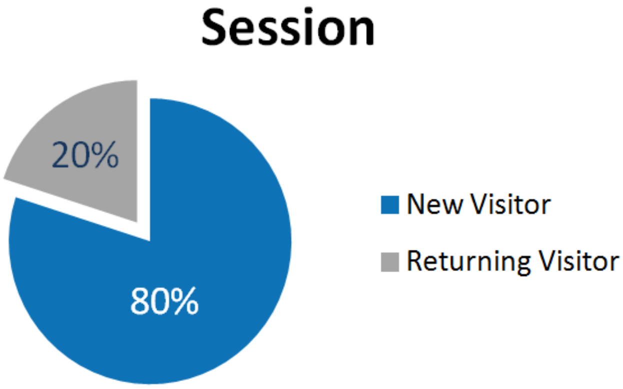


Figure 4: PRACTICE website statistic of the distribution of the type of the visitors

Considering the top downloaded documents during the second project period, the deliverable D31.1 "*Risk assessment and current legal status on data protection*" was the most frequently viewed/downloaded document of the PRACTICE website, as shown in Figure 5. Since the publication of the second issue of the PRACTICE newsletter in July 2014 this document was downloaded 3,482 times, being the second most viewed PRACTICE document. This is followed by the third issue of the PRACTICE newsletter (published in March 2015) with 2,365 hits. Also two papers which were published by project partners with the title "*TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits*" and "*Compact Ring-LWE Cryptoproce*ssor" prove notable hits.

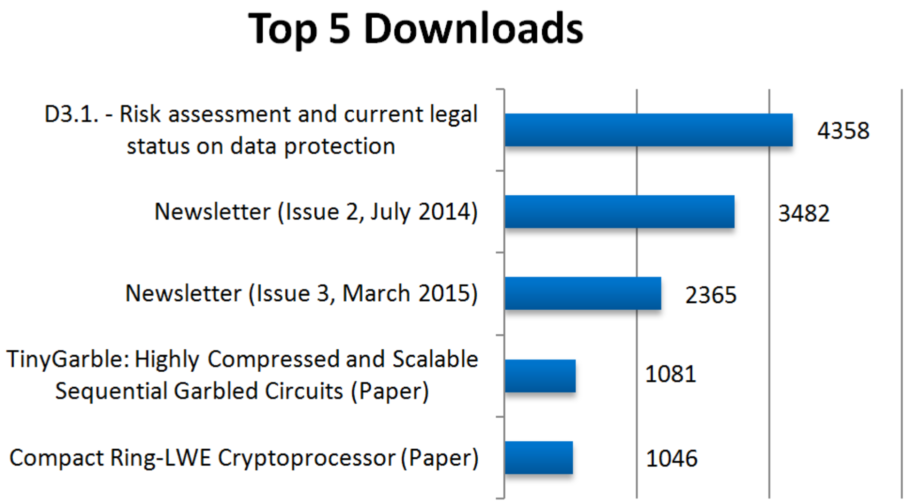


Figure 5: PRACTICE website statistic of the most frequently viewed/downloaded documents

1.2.3.3 Restricted area of PRACTICE website

As explained in D32.1 there is a password-protected area which is reserved for project participants in order to share project-internal data only. The documents and information as well as especially the Calendar were updated on a regular basis. The calendar includes the following categories:

- Meetings, Conferences, Workshops, etc.
- Telephone conferences
- Deliverables & Milestone Submission
- Interim Management Report

By using this calendar the PRACTICE consortium is always aware of upcoming meetings, conferences, workshops or telephone conferences as well as deadlines of upcoming deliverables, milestones and the interim management reports.

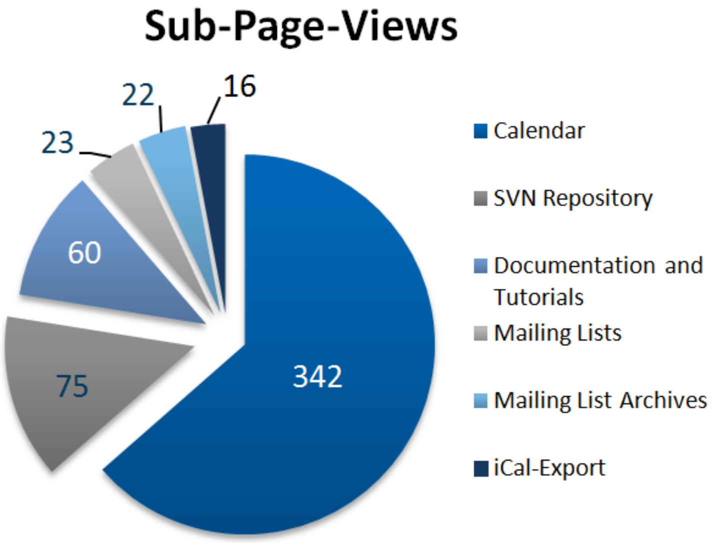


Figure 6: PRACTICE website statistic of the sub-pages within the restricted area

1.2.3.4 Analysis of the website

As reported above, website statistics allow to easily give numbers for both indicators that have been selected as KPIs, that are “**Number of visits**” and “**Number of unique visitors**”. As the metrics that measure success of a website are not universally recognized, we selected 10 as number of daily visits amounting to a target value of 3650 visits per year and 5 for number of unique visitors, amounting to 1825 unique visitors. Both thresholds have been easily overcome, testifying the fact that the website is easily reachable, and the project attracts interested people involving both researchers and general public.

1.2.3.5 Publication of other results

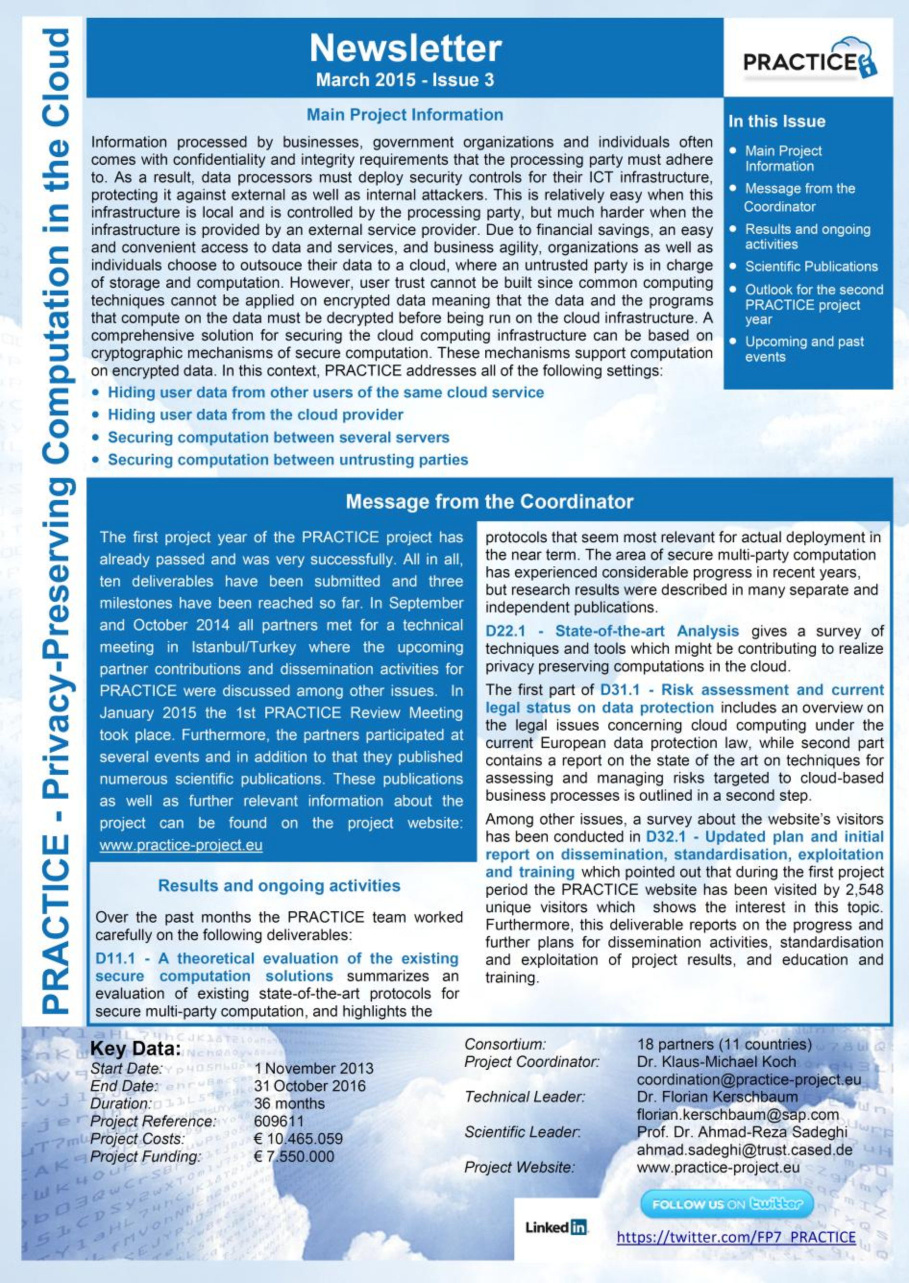
All presentations to the general public are listed in an action overview list and are updated by the partners on a regularly basis. The project was presented to the general public also via the PRACTICE website during the second project year.

Type of activities	Main leader	Title	Date			Place	Type and goal of the event	Countries addressed
			Day	Month	Year			
Web	TEC, ALL partners	PRACTICE Newsletter Issue 3		3	2015	Online	Newsletter can be downloaded from PRACTICE website	International
Web	PAR	PRACTICE Secure Survey Platform		6	2015	Online	Several deployments of the platform are available on the PRACTICE website	International
Web	CYBER	Sharemind SDK		6	2015	Online	Tools for creating privacy-preserving apps and services can be downloaded	International
Web	INESC TEC	ADSNARK implementation		9	2015	Online	The source code of the ADSNARK implementation that gave rise to the IEEE S&P publication was added as a contribution to the libsnark open source cryptographic library	International

Table 4: Dissemination activities

1.2.3.6 Project newsletters

In the first half year of the second project period (M17), a newsletter of the PRACTICE project was launched in order to address project related news (Figure 7). Furthermore, the newsletter offers current information and disseminates important events. The newsletters can be found on the PRACTICE website and are also posted via the PRACTICE Twitter and PRACTICE LinkedIn account to catch further public awareness. It is planned to publish newsletters on a regular basis, in order to keep external partners and the public updated.



PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

March 2015 - Issue 3

PRACTICE

Main Project Information

Information processed by businesses, government organizations and individuals often comes with confidentiality and integrity requirements that the processing party must adhere to. As a result, data processors must deploy security controls for their ICT infrastructure, protecting it against external as well as internal attackers. This is relatively easy when this infrastructure is local and is controlled by the processing party, but much harder when the infrastructure is provided by an external service provider. Due to financial savings, an easy and convenient access to data and services, and business agility, organizations as well as individuals choose to outsouce their data to a cloud, where an untrusted party is in charge of storage and computation. However, user trust cannot be built since common computing techniques cannot be applied on encrypted data meaning that the data and the programs that compute on the data must be decrypted before being run on the cloud infrastructure. A comprehensive solution for securing the cloud computing infrastructure can be based on cryptographic mechanisms of secure computation. These mechanisms support computation on encrypted data. In this context, PRACTICE addresses all of the following settings:

- **Hiding user data from other users of the same cloud service**
- **Hiding user data from the cloud provider**
- **Securing computation between several servers**
- **Securing computation between untrusting parties**

In this Issue

- Main Project Information
- Message from the Coordinator
- Results and ongoing activities
- Scientific Publications
- Outlook for the second PRACTICE project year
- Upcoming and past events

Message from the Coordinator

The first project year of the PRACTICE project has already passed and was very successfully. All in all, ten deliverables have been submitted and three milestones have been reached so far. In September and October 2014 all partners met for a technical meeting in Istanbul/Turkey where the upcoming partner contributions and dissemination activities for PRACTICE were discussed among other issues. In January 2015 the 1st PRACTICE Review Meeting took place. Furthermore, the partners participated at several events and in addition to that they published numerous scientific publications. These publications as well as further relevant information about the project can be found on the project website: www.practice-project.eu

Results and ongoing activities

Over the past months the PRACTICE team worked carefully on the following deliverables:

D11.1 - A theoretical evaluation of the existing secure computation solutions summarizes an evaluation of existing state-of-the-art protocols for secure multi-party computation, and highlights the protocols that seem most relevant for actual deployment in the near term. The area of secure multi-party computation has experienced considerable progress in recent years, but research results were described in many separate and independent publications.

D22.1 - State-of-the-art Analysis gives a survey of techniques and tools which might be contributing to realize privacy preserving computations in the cloud.

The first part of **D31.1 - Risk assessment and current legal status on data protection** includes an overview on the legal issues concerning cloud computing under the current European data protection law, while second part contains a report on the state of the art on techniques for assessing and managing risks targeted to cloud-based business processes is outlined in a second step.

Among other issues, a survey about the website's visitors has been conducted in **D32.1 - Updated plan and initial report on dissemination, standardisation, exploitation and training** which pointed out that during the first project period the PRACTICE website has been visited by 2,548 unique visitors which shows the interest in this topic. Furthermore, this deliverable reports on the progress and further plans for dissemination activities, standardisation and exploitation of project results, and education and training.

Key Data:

Start Date:	1 November 2013
End Date:	31 October 2016
Duration:	36 months
Project Reference:	609611
Project Costs:	€ 10.465.059
Project Funding:	€ 7.550.000

Consortium:	18 partners (11 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@practice-project.eu
Technical Leader:	Dr. Florian Kerschbaum florian.kerschbaum@sap.com
Scientific Leader:	Prof. Dr. Ahmad-Reza Sadeghi ahmad.sadeghi@trust.cased.de
Project Website:	www.practice-project.eu

FOLLOW US ON twitter

LinkedIn

https://twitter.com/FP7_PRACTICE

Figure 7: PRACTICE newsletter issue 3

1.2.3.7 Analysis of the newsletter/posters

The success of the dissemination activities related to the publication of newsletters, posters and leaflet can be measured by reporting as KPI the "Number of contacts" and the "number of downloads". The values registered for those activities are reported in the table below. The threshold values selected are 100 for contacts and 100 for download. Both limits have been easily overcome, meaning that those channels are being efficiently used and the dissemination goals are being achieved.

Document	Downloads
Newsletter (Issue 1, March 2014)	757
Newsletter (Issue 2, July 2014)	4,214
Newsletter (Issue 3, March 2015)	2,365
Announcement-Letter	517
Poster	561

Document	Downloads
Roll-Up	398
Leaflet	479

Table 5: Number of contacts for posters, newsletters and leaflets

1.2.4 Social media: PRACTICE Twitter account and PRACTICE LinkedIn group

Making use of the advantages of social media helps spreading project information to a large audience. As a consequence, they are valuable means to disseminate project ideas and results.

Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". So far we have tweeted 33 entries and have 43 followers. We will continue with monthly tweets to inform the interested community about the latest project news and increase the number of followers. At the next conferences, presentations and given talks we will continue to inform the audience to follow us on Twitter. The PRACTICE project is available on https://twitter.com/FP7_PRACTICE

LinkedIn is a social networking site for people in professional occupations or simply a social network for business. The PRACTICE group is a closed group with currently 55 members. This ensures that only people who have been approved by the manager or admin can see the content of the group. It can be accessed via http://www.linkedin.com/groups?gid=6553977&trk=anet_about_guest-h-parent_group

1.2.4.1 Analysis of the social media

Social Network	#
Twitter	33 tweets 13 tweets within this project period 43 follower
LinkedIn	55 members
Blog	14 entries 7 entries within this project period

Table 6: Number of contacts for social networks

The success of the dissemination activities related to the social media can be measured by reporting as KPI the **"number of contacts"** and the **"number of posts/message"** as shown in Table 6. The first KPI, related to the number of contacts (or followers for Twitter) has been overcome for the LinkedIn group, while the number of Twitter's followers is below. As regards the number of posts, whose threshold has been set 2 per month for a total of 24 posts/messages, we register that the number of tweets is sufficient, while the number of messages on the blog is under the threshold.

To improve the use of social media channels, we revised our strategy and decided to augment the number of messages requesting a more active participation of the partners in increasing the number of contacts and the number of posted messages. We plan to better report project's activities by having at least one post produced by each partner, and have at least 2-3 messages per month, with an optimal threshold of one post per week (apart the holidays periods). This strategy could allow a better diffusion of project's activities over these channels.

1.2.4.2 Cooperation with other projects

As part of PRACTICE project management and dissemination activities, further projects in the same area have been identified and the project management team at TEC provided them with the most important information on the PRACTICE-project: http://www.practice-project.eu/links

All cooperations with other projects are listed in an action overview list and have been updated by the partners on a regular basis. Currently 7 cooperations have been established during the second project year.

Actual/ planned date (dd.mm.yyyy)	Place	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)	PRACTICE partners involved
April 2015	Online	link related projects to our PRACTICE website	H2020 project SUPERCLOUD	international	all
May 2015	Online	link related projects to our PRACTICE website	FP7 project Cumulus	international	all
June 2015	Online	link related projects to our PRACTICE website	FP7 project UaESMC	international	all
June 2015	Tartu, Estonia	Proposal to conduct Tartu city government employee satisfaction survey with PRACTICE survey system.	Tartu city government	Estonia	CYBER
August 2015	Lesbos, Greece	COINS Research School of Computer and Information Security invited to the summer school on Cloud Security. COINS added the PRACTICE summer school to the list of recommendations for the students in their network.	COINS Research School of Computer and Information Security	International	all
September 2015	Bucharest, Romania	SUPERCLOUD partners participate in PRACTICE summer school and give talks	H2020 project SUPERCLOUD	international	all
Y2	E-Mail	distribution of newsletters	Projects listed on website and AB members	international	all
October 2015	Porto, Portugal	Kickoff meeting of the SafeCloud H2020 project included a participation of INESC TEC and CYBER, which are also partners in the PRACTICE project. Results of PRACTICE were presented and discussed as starting point for the work in this new project.	H2020 project SafeCloud	international	INESC TEC, CYBER

Table 7: List of cooperation with external organisations or other projects/programmes

Chapter 2 Standardisation

PRACTICE standardisation activities have the goal to introduce the technologies developed within the project mainly related to encrypted computation in the cloud into standards, so that the results and the products can be more favourable accepted and early adopted by interested stakeholders.

2.1 Standardisation strategy in M13-M24

One of the main focus areas is to allow processing on encrypted data wherever possible. Unlike today's processing of clear data, this substantially decreases the risks of privacy and confidentiality exposures by leakage of sensitive or privacy invasive data.

The initial goal of our standardisation activities is to promote the PRACTICE approach. In year 2, we now started advertising specific PRACTICE results to the corresponding standardisation bodies. While the technology is still evolving, the focus of our first standardisation efforts where we participated was to promote privacy of cloud-based services in order to increase the commercial demand for the PRACTICE technologies.

Additionally, we are contributing to technical standards to enable interoperability of new cryptographic technologies developed and applied in PRACTICE.

2.1.1 ISO/IEC JTC 1 SC 27

The sub-committee 27 of ISO/IEC Joint Technical Committee 1 works in information security topics. We contribute to two working groups:

Working Group 2 (Cryptography): in this WG, we are contributing to fundamental standards on homomorphic cryptography, a foundation of most PRACTICE technologies.

Working Group 5 (Privacy and Identity Techniques): here, we contribute to standards that describe risk assessment and privacy-enhancing technologies. Our goal is to make technologies developed in PRACTICE more desirable to governments and industry internationally.

For technology standardization, we have chosen ISO/IEC over CEN/CENELEC, because technical standards are international by design. Similarly, we are motivated to disseminate the European privacy culture to other areas in the world.

2.2 Standardisation results in M13-M24

In the following we report on the specific activities executed during the 2nd year of PRACTICE, including the two main standardization areas described in Sec. 2.2.1 and Sec. 2.2.2, and the individual standardization plans presented by the partners in Sec. 2.3.

2.2.1 ISO/IEC JTC 1 SC 27

In March 2015, PRACTICE sent a liaison statement to SC 27, with thorough new comments on the two-part secret sharing project (ISO/IEC 19592). Secret sharing remains a key enabling technology of PRACTICE secure computation capabilities. Thus, it also remains a target technology for standardization.

Baldur Kubo, acting liaison officer participated in the SC 27 meeting in Malaysia to oversee the editing session for ISO/IEC 19592 and identify projects that PRACTICE should be contributing to in the future.

Our proposals were successful and our comments were accepted as follows.

1) ISO/IEC 19592 Secret Sharing – Part 1: General. 16 comments,16 accepted.
2) ISO/IEC 19592 Secret Sharing – Part 2: Fundamental mechanisms. 35 comments, 34 accepted, 1 technical comment rejected.

The strong acceptance rate for a high number of comments signifies a strong impact to the standards.

In August 2015, PRACTICE sent a new liaison statement, showing its interest in two upcoming projects:

1) New Work Item Proposal for Privacy enhancing data de-identification techniques. This project will directly enumerate technologies that protect data during processing and PRACTICE will ensure that the highly secure technologies developed in Europe are included in the international standard.
2) Study Period for a Privacy Engineering Framework. PRACTICE sent five comments to the study period, voicing its concerns over an unclear scope. However, as some the current proposals in the project have been from the EU FP7 PRIPARE project, we are actively looking for ways to collaborate and support them in their goals.

Dan Bogdanov will participate in the SC 27 meeting in Jaipur in October as the liaison officer from PRACTICE.

2.2.2 Privacy standardisation at the world wide web consortium (W3C)

Matthias Schunter (INTEL) has continued to act as one of three co-chairs of the W3C Tracking Protection Group (http://www.w3.org/2011/tracking-protection/).

The World-wide Web Consortium standardises all basic web technologies such HTTP, HTML, XML, and CSS. It is an open forum that aims at the evolution of the future web.

At this time, there are two key initiatives underway:

- W3C Tracking Protection Working Group (“Do Not Track”): This working group aims at providing an opt-out from tracking to end users. This includes two parts: To standardise a protocol to transmit user preferences and to define what privacy-enhancing changes should be made by web-sites receiving this signal.
- User-centric Privacy: The W3C is currently investigating how enhanced control over their privacy can be provided to end users. To achieve this, W3C is conducting a public hearing (Nov 2014) to collect inputs from the community including PRACTICE.

An important observation is that most web- and mobile services are implemented as cloud services. Our goal when participating in these standardisation committees is to ensure that privacy requirements from the project and the EU are addressed. In turn, this will increase the demand for privacy-enhancing technologies such as the PRACTICE technologies.

For year 2 of PRACTICE, our goal when chairing the TPWG was to progress the technical specification (Tracking Preference Expression) into CR status (candidate recommendation) while progressing the policy specification (Tracking Compliance) to LC (last call).

The Tracking Preference Expression has reached Last Call end of 2014 and is now in the “Candidate Recommendation” state where stakeholders are asked to implement the standard. The next step will be a formal call for implementations.

Note that this standard is already widely adopted. All major browsers (Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, Apple Safari) have implemented a tracking preference that allows their users to opt-out using the TPE protocol that is co-sponsored by PRACTICE.

In 2015, the W3C Do Not Track group resolved the pending issues for the Tracking Compliance document and published this document as a Last Call draft. At this time, all stakeholders are invited to review this draft, give feedback, and propose changes. To reach this state, the working group has resolved hundreds of issues.

2.3 Per-partner standardisation plans for M13-M36

Partners have been asked to update their standardisation plans published within Annex I – Description of Work, if necessary.

TEC`s standardisation plans haven't changed so far. As coordinator, TEC actively supports the standardisation activities of the consortium and provides assistance where needed and appropriate. Furthermore TEC is the interface between the Standardisation Institute and the partners.

TUDA has been leading several international research and development projects on design and implementation of trustworthy computing platforms and trusted computing, security hardware, and particularly Physically Unclonable Functions (PUF), Cryptographic Privacy-protecting Systems, and cryptographic compilers (in particular for secure computation). The experience gained in PRACTICE will be managed within TUDA in order to increase the knowledge amongst the group members. The key person from TUDA, Prof. Sadeghi, has been awarded with the renowned German award “Karl Heinz Beckurts” for his research on Trusted Computing technology and its transfer to industrial practice. The acquired knowledge from PRACTICE will help TUDA make further industrial innovations. TUDA will support different future projects realizing secure computation in systems or use-cases based on the technological developments and findings of PRACTICE.

CYBER will continue to disseminate PRACTICE results in ISO/IEC JTC 1 SC 27.

INTEL plans to continue to chair the W3C Do Not Track working group. Our goal is to push the current draft documents to their next formal state (recommendation for TPE and last call for TCS) while implementing a sound balance between privacy and efficiency of the implementation. One important goal will be to promote privacy-enhancing technologies as one enabler of this balance.

UMIL is involved in the activities of the CEN/WS RACS (CWA 16871-1:2015) (European Committee for standardization) workshop “Requirements and Recommendations for Assurance in Cloud Security (RACS)”, which has been started in 2014 by a group of stakeholders including some partners of CIRRUS FP7 project, including the National Standardization Bodies of 33 European countries. The workshop goal is to present a comprehensive overview on regulatory and standardisation activities related to cloud computing, including representative samples of ICT technical specifications developed by fora and consortia as well as recommendations for best practice and technical specifications on monitoring and certifications of cloud computing services. Practically speaking, CEN/WS RACS is using the findings of several projects funded by the European Commission to provide a set of recommendations for cloud assurance. CWA-RACS has obtained liaison status with the ISO 27009 standardization. Ernesto Damiani (UMIL) appointed as the chair of the WG, leading the influencing effort of CEN/WS RACS on ISO 27K standardisation process, in strict cooperation with CIRRUS.

RACS business plan is composed of three main milestones corresponding to three main specification release:

1) "Requirements and Recommendations for Assurance in Cloud Security – Part 1: Contributed recommendations from European projects" [CONCLUDED]
    - This first part gave recommendation on Security Requirements/Properties Document based on the survey about missing cloud security requirements and controls (versus 27001)
2) "Requirements and Recommendations for Assurance in Cloud Security – Part 2: Requirements for the future security control frameworks in a certification context" (ONGOING)
    - The second part is focusing on guidelines and solutions for evidence collection and assurance.
    - An online meeting on the status of the workshop and of document part 2 is scheduled for October 2015.
3) "Requirements and Recommendations for Assurance in Cloud Security – Part 3: Analysis of the relation with ISO/IEC 27017 CC"
    - The third part will depend on the evolution of the ISO 27017 standards and on available resources.

A final version of the first document "Requirements and Recommendations for Assurance in Cloud Security – Part 1: Contributed recommendations from European projects" has been released on March 25th, 2015 and will be the basis for the further discussion in the ISO 27017 forum.

Chapter 3 Exploitation

Exploitation is recognised as the key enabler for the success of the PRACTICE project. Hence, all PRACTICE 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.

Wherever possible, research results will be used for the creation and support of new products and services. These products and services will lead to a competitive advantage of the participating organisations and will substantially contribute to the benefit of the targeted constituents. In order for the exploitation to be effective, an integrated approach will be necessary, combining experience and expertise from the development department and solution management, and the involvement of a user base represented by the consortium partners and industrial contacts.

3.1 Exploitation in M13-24

In this section, we report on the exploitation activities performed by the partners in the 2nd year of the project, presenting some success stories in section 3.2, and the individual updated exploitation plans in section 3.3.

3.2 Exploitation stories

PRACTICE research results have already been exploited by some of the partners to develop some products or perform some activities, resulting in tangible outcomes of the participation to the project. Here we report some of the most successful experiences.

3.2.1 SAP

In 2012 SAP Security Research started its internal advanced development project SEEED – Searching over Encrypted Data. Its goal was to build a prototype of an advanced system of client-controlled database encryption. The recent developments in academia – such as MIT's CryptDB – spurred the interest of industry and led to a significant advancement of the state-of-the-art. The SAP team set out to investigate the gaps to commercial deployment and incremental fill these. Hence, the exploitation strategy was one of "theory to practice" where the SAP team was leading the bridge.

The prototypical development and customer interaction phase was a continuous learning process. The problems crucial in deployment, such as integration or on-boarding, are often overlooked in scientific research. The SAP team invented and implemented a number of ground-breaking approaches in this area.

Later, the SEEED project gathered significant internal attention within SAP. Several discussions with stakeholders – including at the top executive level – took place. The team was 1st runner-up within the development organization for the internal Hasso Plattner's Founders Award. After these initial discussions teams – including product groups, central security and security research – where formed to define the product roadmap. Following an internal alignment process – including again top-level executives – these roadmaps were finalized. We expect corresponding product announcements from SAP in the foreseeable future.

The PRACTICE project was instrumental in the success of the SEEED project. It provided the financial support to develop crucial extensions to the prototype which would have not been feasible without it. The exchange with external partners on client-controlled cloud encryption – as spearheaded by PRACTICE – provided valuable insights and influences. We were able to develop a number of high-profile contributions to the scientific community and internal intellectual property that secure SAP's leadership in the space of property-preserving encryption. Overall, the SEEED project – with the support of PRACTICE – is a success story of commercial exploitation of a research technology, but also PRACTICE is a success story of an approach of integration of public-funded projects into internal advanced development projects. A model SAP is continuing to pursue with the ESCUDO-CLOUD and TREDISEC projects.

3.2.2 PARTISIA

Partisia's approach to exploitation is basically all about developing MPC applications in collaboration with business partners and include investors and other business competences when necessary. The two spinouts from Partisia, Energiauktion.dk and Sepior, is a result of this approach to exploitation. The idea and purpose with this exploitation strategy is for Partisia to remain agile and open to business partners and yet commercially focused.

The spinout Sepior underpins this exploitation strategy. The commercial focus on "Key-Management-as-a-Service" based on MPC has made it possible to include capital and business partners without preventing Partisia in pursuing other applications of MPC. Sepior is now scaling up thanks to private investors and other funding including a SME Instrument phase 2 grant.

Partisia's participation in PRACTICE is aligned with this exploitation approach. Here we try to include end users and potential business partners in the prototype development as much as possible. The developed survey system which is an application that is easy to relate to, is now used to show case the technology. Also, the fact that the survey system can run on both Sharemind and Fresco/SPDZ is an important signal to end users by addressing the risk of being too locked into service providers.

However, the confidential benchmarking application is the application that involves most end users and business partners. This application involves several banks, a consultancy house and other financial organisations. The application is general and can be used to sell the idea of using MPC in statistics more generally.

The whole focus on secure statistics in PRACTICE has opened up for new exploitation opportunities supported by a grant from the Danish industry foundation. The grant support a project called Big Data by Security, which complement PRACTICE and facilitate more end user involvement. The project aims at practical use of MPC and two specific cases. The first case involves a P2P crowd lending site and MPC will be used to include more confidential information in the credit rating. The second case is collaboration with Danish Statistics and it aims at making sensitive data available for private firms by the use of MPC. Both cases are highly complementary to the work in PRACTICE and facilitate more exploitation of secure statistics based on MPC.

3.2.3 CYBER

Cybernetica's exploitation activities in 2015 focused on using PRACTICE technologies to tell good privacy stories. The three noteworthy success stories follow.

First, **CYBER** built a mobile location sharing application that used PRACTICE technologies to hide the user's location. This prototype was demonstrated at the Real World Crypto conference in London in January 2015 with over a hundred uses. The application successfully demonstrated how to integrate secure computing into a mobile app and run the backend on the cloud. **BIU** and **PAR** assisted in hosting the system.

Second, **CYBER** continued the development of tax fraud detection prototype following the suggestions from the first Advisory Board meeting. The AB suggested that we evaluate the feasibility and cost of the tax fraud application in actual cloud deployments. Inspired by that and with generous support from our AB members, we were able to build and deploy a new prototype that reduced the running cost of the application over a hundred times. These results were considered most impressive by the Advisory Board and also outside parties. We are now exploring ways of replicating this success with other applications and offering it as a capability to the public.

CYBER formed a collaboration with the city government of Tartu to run the governments employee satisfaction survey using the PRACTICE cloud-based secure survey system (joint development of **CYBER** and **PAR**). The survey is set to run in October 2015, with an analysis running into November 2015. Once completed, the study will be yet another demonstration of a cloud service with unparalleled privacy guarantees. To summarize – the cloud-based privacy-preserving survey system in PRACTICE has seen a lot more real-world use than initially planned. E.g., **CYBER** is consistently using it internally and it was also used by WP24 in PRACTICE.

CYBER published a preliminary version of the SDK that was downloaded and tested internationally. People registered for updates across the world and we got good feedback for improving its precision and usability.

3.3 Per-partner exploitation plans

Every partner has been asked to update the exploitation plans published within Annex I – Description of Work and provide an initial report of the performed exploitation activities within year 2 of the PRACTICE project.

Partner 1: Technikon Forschungs- und Planungsgesellschaft mbH (TEC) – Austria	
Report on exploitation activities after 2nd project year	We have developed a secure survey ("doodle") application prototype, which provides a solution to participate on a survey/poll without revealing private inputs. This has been done by using PRACTICE technology for encryption and decryption of the users voting as well as for the computing of the overall result. The voting system is based on Fully Homomorphic Encryption Scheme (FHE), which allows operations on a ciphertext without encrypting it first. As a result data is processed in a secure and anonymous way without revealing the users privacy, even when a statistic is published to the public. During the 2nd year we have enhanced our knowledge in security & privacy of cloud applications by researching secure interfaces for cloud computing platforms. Furthermore, TEC continued to provide results to our customers through the project website and triggered their interest for the PRACTICE security technology.
Updated exploitation plan after 2nd project year including stakeholder	**TEC** has the proficiency as industrial security service provider to use and re-use project results within our regular business lines. Technikon will follow up on the researches of the usage of PRACTICE concepts for our technical platforms, our trusted knowledge suite, and providing enhanced collaboration tools, web site, servers, etc. for our current and future customers. Within our security services the use-case concepts of PRACTICE can directly be applied within our security concepts and solutions, once the industrial needed maturity of the results have been reached.

Partner 2: SAP AG (SAP) – Germany	
Report on	In the second year the plan was to create demand and a roadmap for the

Partner 2: SAP AG (SAP) – Germany	
exploitation activities after 2nd project year	developed cloud encryption solutions. Therefore, we held meetings with several potential customers and internal stakeholders in product development, presented at SAP's Security Advisory Board, and engaged in the political debate dealing with data protection regulation (whether encrypted data is handled as personal identifiable information). In total, our results regarding the exploitation for PRACTICE are as follows: • We held meetings with several pilot customers, presenting tools for processing encrypted databases. The development of these tools benefits directly from our collaboration in PRACTICE. • We held meeting with several product development groups for core products as well as specific cloud offerings. We defined clear strategies for product integration and product roadmaps. • We introduced future technologies derived from tools developed in PRACTICE at SAP Product Security Expert Summit 2015 to all internal stakeholders of information security. • In order to shape SAP's future regarding security and privacy we presented at the Security Advisory Board of SAP introducing the encryption concept to receive further advice on maximizing the customer benefit. • We consulted the European Parliament concerning the data protection regulation.
Updated exploitation plan after 2nd project year including stakeholder	Recently **SAP** has announced its preliminary financial results for the third quarter of the year 2015. SAP has reported strong growth in the cloud, particularly, new cloud bookings – one key measure for SAP's sales success in the cloud, increased 102% in the third quarter. This underpins the importance of cloud delivery for the future of SAP and consequently puts security into the strategic focus of SAP – in more detail, we expect secure cloud applications and encrypted databases as key elements for SAP's continuous growth in the cloud. We will therefore continue with the previously developed exploitation plan and concentrate on our schedule for the 3rd year, namely "initiate transfer": Create a detailed transfer plan and intend to hand over the developed code.

Partner 3: Technische Universitaet Darmstadt, Intel Collaborative Research Institute for Secure Computing (TUDA) – Germany	
Report on exploitation activities after 2nd project year	In the second year, TUDA published several research papers at 5 of the top 6 conferences for security & privacy. We made many of our prototype implementations available as open-source projects, e.g., at http://encrypto.de/code. We presented our results on "practical private set intersection" to an industrial audience at the booth of the BMBF (German ministry for research and education) at the exhibition CeBIT 2015. Summer School on Secure and Trustworthy Computing, Bucharest, Romania, September 23 – 27, 2015: 18 speakers provided a large spectrum of theoretical and practical aspects associated to secure and trustworthy computing: Secure multi-party computation, searchable encryption, hardware security and new trends (Intel's SGX), runtime attacks (return oriented programming), cloud computing scenarios like the European cooperative research project SUPERCLOUD. Over 70 participants from 10 countries attended the event. All responses were enthusiastic about the content and the overall quality of the Summer School. We received excellent feedback from the participants and are planning to do it next year as well.
Updated exploitation plan after 2nd project	The exploitation plan for the next year will focus on further showing practicality of secure computation technologies by means of top publications and prototype implementations. In the winter term 2015/16 we

Partner 3: Technische Universitaet Darmstadt, Intel Collaborative Research Institute for Secure Computing (TUDA) – Germany	
year including stakeholder	are offering a seminar on "privacy preserving technologies" in which students learn about techniques developed within the PRACTICE project. Moreover, we are planning to acquire new projects in the area of privacy enhancing technologies.

Partner 4: Alexandra Institutte A/S (ALX) – Denmark	
Report on exploitation activities after 2nd project year	In the second year of PRACTICE, ALX worked on an improved platform for general secure computation based on our internal FRESCO framework and architectural ideas developed within PRACTICE. We also continued work on a financial benchmarking prototype using secure computation and contributed to the secure survey prototype developed by CYBER and PAR.
Updated exploitation plan after 2nd project year including stakeholder	In the third year of PRACTICE **ALX** plans to continue many of efforts we worked on in the second year. This includes improving all of the software mentioned in the second year report. Particular the financial benchmarking prototype is to be delivered in year three, and an improved version of the deployment tool is planned. Additionally we plan to use the new platform developed in the second year to help us implement new secure computation protocols developed by the PRACTICE partners.

Partner 5: Arçelik A/S (ARC) – Turkey	
Report on exploitation activities after 2nd project year	Arcelik has continued to share potential outcomes of PRACTICE project internally in its group of companies informing the potential users. Arcelik also has informed its suppliers about the PRACTICE project during bilateral meetings throughout the second year. PRACTICE project poster were shown and brochures were distributed at Arcelik stands in a number of events during the second project year including NESSI Members Day, Big Data Networking Days, Net Futures, Innovation week in Izmir, Istanbul and a number of H2020 Workshops and Conferences in Turkey. The interested stand visitors have been informed about the project and potential outcomes during these events.
Updated exploitation plan after 2nd project year including stakeholder	**Arcelik** is planning to present PRACTICE project at the Koc Technology Board event "Technology Day" on the 4th of November in 2015 showing potential outcomes and exploitation possibilities to inform Koc Group of companies active in car manufacturing, energy, finance and agri-food sectors. Arcelik's suppliers will be also informed about the project progress and if possible demonstrators will be shown during annual supply chain event in 2016. Finally, Arcelik is planning to show PRACTICE poster, distribute brochures and show demos if possible at its stand in events, trade shows where Arcelik will participate throughout the 3rd year.

Partner 6: Bar Ilan University (BIU) – Israel	
Report on exploitation activities after 2nd project year	In the 2nd year of the project BIU performed research that was presented at the leading security and cryptography conferences. In addition, we continued developing and updated the SCAPI software library to support the most advanced up-to-date secure computation protocols. We have also organized the 5th BIU winter school on cryptography, which focused on practical secure computation. The school lasted for 4 days and had about 150 participants.
Updated exploitation plan after 2nd project year including	In the 3rd year of the project we will focus most of our efforts on further developing advanced secure computation protocols, and continuing to update the SCAPI software library, based on the observations and conclusions in the first two years of the project. We will also run the 6th BIU winter school, which will focus on cryptography in the cloud – verifiable

Partner 6: Bar Ilan University (BIU) – Israel	
stakeholder	computation and special encryption.

Partner 7: Cybernetica AS (CYBER) – Estonia	
Report on exploitation activities after 2nd project year	In Year 2, **CYBER** directed its efforts in PRACTICE at building impressive prototypes to increase the uptake of technologies, following the exploitation plan and also embracing new opportunities. The success stories of the cloud-based privacy-preserving mobile location app and the survey system have encouraged us to start planning the implementation of further privacy-preserving mobile/web applications. The success of cloud-based privacy-preserving tax fraud detection has created a strong interest against CYBER's Sharemind platform and CYBER is already investigating potential commercial usage of the technology.
Updated exploitation plan after 2nd project year including stakeholder	Inspired by successes in 2015, **CYBER** will continue to simplify the deployment of secure computation technology on the cloud to make the technology easier to exploit and scale up its usage in real-world applications. This will include integration with the PRACTICE SDK. **CYBER** will also continue to pursue real-world applications based on successful demonstrations.

Partner 8: Julius-Maximilians Universitaet Wuerzburg (UWUERZ) – Germany	
Report on exploitation activities after 2nd project year	**E**xploitation activities of **UWUERZ** in the 2nd year were focused on two areas: For one, the contact with companies that could benefit from PRACTICE results and on the other hand our teaching activities where we raise awareness for PRACTICE ideas amongst the future generation of decision makers. We contacted about 30 national and international companies mainly from mechanical engineering sector to evaluate current practices of maintenance based on condition data. We discussed related privacy issues and pointed out that our PRACTICE project is developing the infrastructure and applications to overcome these problems. We held a seminar named *Supply Chain Collaboration* that raised awareness for privacy issues and PRACTICE activities. Four master's theses related to PRACTICE contents were completed. Besides, we submitted one paper to a high ranked journal operations research journal and one to the major German conference on business information systems. Both with the potential to spread PRACTICE results amongst the scientific community.
Updated exploitation plan after 2nd project year including stakeholder	In addition to the ongoing work with partnering companies and with our students, members of the **UWUERZ** team will present PRACTICE results related to supply chain management at the *INFORMS* and the *MKWI*. We will submit a paper on “Secure Supply Chain Collaboration” to a special edition of the operations research journal *Interfaces*.

Partner 9: Intel GmbH (INTEL) – Germany	
Report on exploitation activities after 2nd project year	We have prototyped the scalable protocols developed in PRACTICE and have advertised our approach to different Intel stakeholders. We believe that the protocols will allow increased scalability of our IoT systems. Based on PRACTICE results, we gave a course to our IoT business unit to further raise awareness of the privacy-technologies available today.
Updated exploitation plan after 2nd project year including	**INTEL`s** goal for year 3 is to obtain buy-in from a product group to adopt the protocols that we developed in PRACTICE. To foster this, we will investigate hardware security support and further extensions of those

Partner 9: Intel GmbH (INTEL) – Germany	
stakeholder	protocols. Furthermore, we will continue to conduct workshops with customers and Intel stakeholders to promote the results of PRACTICE.

Partner 10: Katholieke Universiteit Leuven (KU LEUVEN) – Belgium	
Report on exploitation activities after 2nd project year	In the second year KU Leuven has published two project-related papers in the top hardware security venue CHES and one paper at DATE. These results have been further disseminated at seminars, lectures, and industrial events. KU Leuven is in the process of extending the results on hardware-assisted SHE and introducing further hardware optimizations. KU Leuven has also conducted collaborations with other research institutions from the project network.
Updated exploitation plan after 2nd project year including stakeholder	**KU Leuven** envisions further collaborations on developing MPC solutions with improved efficiency. The main focus will be on optimizing existing solutions both in practical and theoretical terms. Additionally, we plan to integrate some of the software and hardware code into open source libraries. The main goal, however, is the dissemination of our results in conference and journal proceedings. KU Leuven plans to work on some of these topics with project partners, such as UNIVBRIS and BIU.

Partner 11: INESC PORTO – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC Porto) – Portugal	
Report on exploitation activities after 2nd project year	Collaboration with PRACTICE partners has led to the identification of a use case for verifiable computation in the area of smart metering, which has been pursued in parallel with a nationally funded project in the area of SmartGrids. This has led to a publication in the IEEE Symposium on Security & Privacy. SafeCloud H2020 application was selected for funding and the results of the PRACTICE project are being considered as starting point for SafeCloud development.
Updated exploitation plan after 2nd project year including stakeholder	The last year of PRACTICE will overlap with the first year of the SafeCloud H2020 project. A major part of the **INESC Porto** exploitation plan for PRACTICE is related to ensuring that the know-how and deliverables acquired in this project are taken advantage of in SafeCloud. INESC Porto will also continue to be actively involved in dissemination via scientific publications, participation in industrial events, and training activities.

Partner 12: Aarhus Universitet (AU) – Denmark	
Report on exploitation activities after 2nd project year	In the second year AU has published papers at major cryptographic conferences presenting results obtained in the project. The cooperation with other partners in the project helped in identifying some interesting research direction.
Updated exploitation plan after 2nd project year including stakeholder	In the third year **AU** will continue to investigate the possibility of designing more advanced cryptographic protocols, with focus on tools and protocols to deal with malicious adversaries. In particular AU plans to work with CYBER towards realizing efficient 2-party protocols.

Partner 13: Technische Universiteit Eindhoven (TUE) – Netherlands	
Report on exploitation activities after 2nd project year	TUE takes part in PRACTICE to extend its research portfolio into secure multiparty computation, and more generally, its research portfolio into privacy-protecting protocols. TUE aims at scientific output, mainly in the form of contributions at workshops and conferences. Furthermore, prototypes as created in PRACTICE will be very useful for demonstration purposes, to show the practicality of secure multiparty computation, and to see how it can be applied in advanced scenarios. These demonstrations will also be used for teaching purposes. In addition, TUE seeks contacts with potential partners from industry and government for projects on applied secure multiparty computation. In particular, TUE cooperates with Philips Research.
Updated exploitation plan after 2nd project year including stakeholder	Our experience and exposure from the PRACTICE project has helped **TUE** to get in contact with potential partners in the Netherlands for future projects in secure multiparty computation (CBS, Philips). Furthermore, we have broadened our research into secure multiparty computation, extending into several directions all connected to verifiability, resulting in several works (finished and in progress). Finally, we have worked on several prototypes, partly relying on VIFF and SCAPI. All these activities reinforce TUE's position as a centre of expertise in secure multiparty computation.

Partner 14: University of Bristol (UNIVBRIS) – United Kingdom	
Report on exploitation activities after 2nd project year	Based on work within the consortium UNIVBRIS has identified several interesting research directions that were materialized in scientific papers published several papers at leading conferences on security and cryptography. Results from PRACTICE formed the basis of the summer school organized together with TUDA.
Updated exploitation plan after 2nd project year including stakeholder	Future work will follow similar lines where we identify interesting research topics relevant to the aspects investigated within the PRACTICE project. In particular, we plan to expand the collaboration with INESC on building protocols based on trusted hardware.

Partner 15: Distretto Tecnologico Aerospaziale S.C. A R.L. (DTA) – Italy	
Report on exploitation activities after 2nd project year	During the second project year, DTA focused its dissemination activities on the direct involvement of the aeronautic firm AvioAero (a member of DTA consortium) into the project activities. In particular, IT and supply chain staff belonging to AvioAero was informally interviewed to verify the relationship between PRACTICE project outcomes and the organizational strategic innovation roadmap. The result is that objective of the firm is to improve its business performance of the MRO business segment by leveraging collaboration opportunities with its customers, that are currently the highest source of criticalities. The approach, the methodology and the expected results of PRACTICE are in line with the innovation agenda of the firm. Moreover, the firm provided significant support to the linked third party UNISA in order to tailor the planning system to its main problems (in example the introduction of penalties role in the planning process). During this year, IT and supply chain staff of other aeronautic firms, member of DTA consortium, were interviewed in order to make them aware of security issues related to the diffusion of cloud systems. Actually, aeronautic firms are moving in this IT sector without a clear strategy, they are pushed from one side by the capability to reduce costs by outsourcing on clouds minor systems and applications and from the other side by the capability to involve other supply chain participants into effective data

Partner 15: Distretto Tecnologico Aerospaziale S.C. A R.L. (DTA) – Italy	
	sharing system. Security concerns affected this trend restraining the involvement of partners to the most tied ones and the business processes innovated through cloud systems (few business processes were taken in consideration), while an effective analysis of business risks and opportunities brought by cloud systems is rarely executed. Part of this activity were executed supporting the survey carried out by UNISA. A third objective achieved in this period is the participation at the ASD Days, an international meeting dedicated to Aerospace, Defence and Security & UAVs (http://www.asddays.com/). The activities and results of DTA and of its linked third party, were presented during the session targeted at European aerospace clusters. The objectives of this presentation were to diffuse information about PRACTICE project and in particular in supply chain system innovations, to attract other European aeronautic actors on the research topic aimed at exploring and innovating risk management in collaborative partnerships, to show competence and capabilities developed in the DTA consortium. The participation in the ASD Days was also an opportunity to present innovation based collaboration practices applied among DTA members and to present the Apulian aerospace system to the European network. Lastly, during this period it was planned to apply the risks analysis methodologies developed into the PRACTICE by UNISA in the project TAKEOFF, participated also by DTA. TAKEOFF project (funded through national funds) is focused on designing and implementing the IT platform for a strategic regional local asset: the test range for UAV (and other aerial systems prototype) based in the Taranto-Grottaglie airport. The IT platform will aimed at offering service to customers of the test range, it will be based on a cloud environment managing flight test data belonging to different customers.
Updated exploitation plan after 2nd project year including stakeholder	The exploitation plan for next year is mainly focused on applying the risk analysis methodology in other collaborative processes carried out collaboratively in the aeronautic supply chain. Moreover knowledge and competence will be also applied in other projects (TAKEOFF firstly). Risk management methodology and security challenges will be object of other research projects and initiatives in order to explore the impact on other collaborative processes.

Partner 16: Università degli Studi di Milano (UMIL) – Italy	
Report on exploitation activities after 2nd project year	In the second year, UMIL has published several paper s in international conferences and journals, and has presented the results developed in to PRACTICE in several events. This has strengthened the position of UMIL as a major educational/research player in the security and trustworthiness of ICT and cloud infrastructures. Many topics covered in PRACTICE have been introduced in courses and used for research thesis.
Updated exploitation plan after 2nd project year including stakeholder	The exploitation plan for next year will focus on further refining and extending the risk analysis methodology, and to develop the tool. The results will be used for producing scientific publications, for teaching purposes, for contacting potentially interested partners and companies and propose new collaborations. Furthermore, collaboration in PRACTICE has broadened the spectrum of research in **UMIL** on secure multi-party computation, opening the way to new projects and proposals of collaboration.

Partner 17: Partisia (PAR) – Denmark	
Report on exploitation activities after 2nd project year	During the second year, PAR's exploitation activities have primarily focused on meetings with stakeholders in the two MPC applications (survey and benchmarking) alongside fundraising aimed at more exploitation. The survey system has been functioning as a useful showcase and the benchmarking system involves several stakeholders directly. As reported in section 3.2.2, a grant from the Danish Industry Foundation will complement PRACTICE and involve more end user and other stakeholders in the coming years.
Updated exploitation plan after 2nd project year including stakeholder	**Partisia's** approach to exploitation by developing MPC applications in collaboration with business partners remains the same. The new project with the Danish Industry Foundation expect to improve the exploitation by including more stakeholders and facilitate a better understanding of the go-to-market strategy for secure statistics. The survey and benchmarking applications will be used to find the right business partners needed to meet the market.

Partner 18: Georg-August-Universitaet Goettingen Stiftung oeffentlichen Rechts (UGOE) – Germany	
Report on exploitation activities after 2nd project year	In the second year, UGOE's exploitation activities have again been focused on the collection and arrangement of materials (cases, articles, books, and the new proposal for a General Data Protection Regulation (GDPR) by the Council of the European Union) as a source for articles, reports and conference proceedings concerning legal problems and solutions regarding the project outcomes. Two articles with the working titles "Encrypted data and the GDPR" and "Joint controllership" are currently being prepared and written.
Updated exploitation plan after 2nd project year including stakeholder	**UGOE** will publish articles in scientific journals (as mentioned above) and take part in legal conferences. The results of research will be disseminated in possible conference proceedings. In addition the results of research will be published and elaborated further in articles in legal journals and reviews. Furthermore UGOE will contribute to dissemination activities of other project partners as far as they relate legal topics.

Table 8: Exploitation reports and updated plans

3.4 Joint exploitation strategies

In addition to the individual exploitation activities mentioned above, the partners performed common exploitation activities as well. The project website was exploitation-oriented upgraded and the PRACTICE results were published. In a further step it is planned to include search engines and optional registration for specific keywords. The PRACTICE partners participated at several security-oriented exhibitions, conferences and workshops, where the results of the project were presented to business stakeholders. These events are listed in section 1.2.2.

Among the many development results, some are publicly available to citizens and future customers. The partners developed a secure survey platform which is available via the following link: https://practice-survey.eu/. Also the Sharemind platform for outsourcing computations on private data was enhanced and integrated into the PRACTICE SDK. Within the Developer Zone of Cybernetica, these tools for creating privacy-preserving apps and services can be downloaded: https://sharemind.cyber.ee/sdk.html. Other development and demonstration efforts, such as the search on encrypted data (continued from the SecureSCM project) are on the path to product and service integration.

PRACTICE partners are dedicated to the technology of computation on encrypted data and based their entire business models on it or extended them in order to sell this technology. Other partners are looking for ways to integrate it into their existing business software. As such, PRACTICE has already achieved major industrial take-up and created significant intellectual property relevant to the industrial business models, which has been pursued in an active (patent filing) and passive (publication) manner. One patent has already been granted.

For the third project year it is planned to improve the transferred activities of research results into development, product, and service organisations of the partners. Continuous analysis of transfer opportunities will be performed and the project will be adjusted if necessary in order to ensure the best possible outcome. Further investigations into the possible economic benefits and impact of the expected research results are planned. We will also continuously evaluate the advancement of the research results against the user requirements/needs throughout the project with the help of the user partners.

Chapter 4 Internal and external training

Following the success of last year's training and education survey, it is our belief that good educational materials can make a positive output from the project. It is for this reason that some effort has been dedicated towards planning for training and education. Therefore, this chapter reports on training and education that have been provided by PRACTICE partners to members and non-members alike.

4.1 Training activities

At this point, the project has been running for 24 months. The architecture of the project and each component has been designed and prototypes are under development. Project members have already acquired a certain level of skills, regarding the specific directions of the components they are in charge of.

Most training is carried along with the progress of the project. Mostly, it is in the form of self-training and learning on the job, as the detailed directions of project members have begun to divert and training on general knowledge has been carried in Year 1. Many individual and non-structured learning activities (researchers learn on-the-job) have been taken. Listening to partner talks at project meetings also helped sharing knowledge and inspiring innovation. Besides the self-training, PRACTICE organized a winter and summer school in order to share relevant and new knowledge with students and other interested people. The talks and presentations given in many conferences and other events (see section 1.2.2) can be also seen as further training activities.

4.1.1 Training at project meetings

In the second year, six project meetings have been organized in order to let members meet face-to-face. During these events, opportunity has been provided to members to share their work, knowledge and skills, and therefore a means of providing training. Meetings have included sessions and talks on different scientific aspects, reporting on the state of the art of methodologies and techniques related to the project's topics and breakout session reserved to specific arguments. Further meetings are planned in the next year and will provide place for further training sessions.

4.1.2 Training at schools

Among the training activities, schools on cryptographic primitives and workshops on more advanced topics have been supported:

- BIU ran the annual winter school on cryptography. The school covered advances in practical multi party computation, and had about 150 participants, Lecturers included Ivan Damgard (Aarhus), Yehuda Lindell (Bar Ilan), Claudio Orlandi (Aarhus), Benny Pinkas (Bar Ilan) and Abhi Shelat (University of Virginia). As last year all lectures were videotaped and are provided free of charge on the web.
- CFEM – Center for Research in the Foundations of Electronic Markets (which include ALX/AU and PAR) in collaboration with CTIC - Center for the Theory of Interactive Computation - have organized a workshop on "New Trends in Mechanism Design". The workshop brought together computer scientists and economists including experts in Secure Multiparty Computation (although the later was not the main focus of this workshop).

- TUDA together with UNIVBRIS organized in cooperation with the University Politehnica Bucharest a Summer School on Secure and Trustworthy Computing from 23 to 27 September, 2015 in Bucharest, Romania. Eighteen speakers provided a large spectrum of theoretical and practical aspects associated to secure and trustworthy computing: Secure multi-party computation, searchable encryption, hardware security and new trends (Intel’s SGX), runtime attacks (return oriented programming), cloud computing scenarios like the European cooperative research project SUPERCLOUD. Over seventy participants from ten countries attended the event. All responses were enthusiastic about the content and the overall quality of the Summer School. The organizers received excellent feedback from the participants and are planning to do it next year as well.

4.2 Training planned

Training activities will be carried on the second year of PRACTICE and will include the following activities:

- Tutorial sessions during the project meetings;
- Workshops and schools: BIU has already planned to run a winter school on cryptography in the cloud – verifiable computation and special encryption, on January 4-7, 2016. The lecturers will be Alexandra Boldyreva, Yael Kalai, Hugo Krawczyk, Benny Pinkas, Eran Tromer, Michael Walfish, and Mor Weiss. All lectures and talks will be videotaped and provided free of charge on the web.
- AU is planning a workshop on Theory and Practice MPC in (tentative dates) June 2016, after the successful editions in 2012 and 2014.

Chapter 5 Conclusion

Dissemination, standardization, exploitation and training, are four key areas of activity for the members of the consortium and for the success of the whole project.

As reported, a large quantity of dissemination activities has been performed during the first two years of the project, corroborated by a good degree of quality. Indeed the scientific publications produced by the partners, have been published in the top conferences and journals of the scientific area, producing a deep impact on the community of interested researchers. Dissemination, performed in most part by the commercial members, have also diffused the project's results in events targeting potential stakeholders or the general public.

As regard standardization, the activities have been targeting international standard bodies focusing on topics and techniques related to privacy in the cloud, aiming for a broader acceptance of the project's results.

Exploitation stories reported by some of the partners, as well as the individual exploitation plans, confirm the effectiveness of the research results produced within the project, and the possibility to produce value by taking advantage of the project's activities.

Finally, training events and workshops have been organized attracting a large number of participants with the goal of sharing new knowledge and the project's results with interested people.