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

D32.3

Final dissemination, standardisation, exploitation and training report

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 / D32.3 / 1.1
Activity and Work package contributing to the deliverable:	Activity 3 / WP32
Due date:	October 2016 – M36
Actual submission date:	8th November, 2016

Responsible organisation:	UMIL
Editor:	Stelvio Cimato
Dissemination level:	Public
Revision:	1.1

Abstract:	This deliverable reports on the project's activities in the area of dissemination, standardisation, exploitation and training which have been executed since M25 until the project end in M36 (see D32.1 and D32.2 which reported about the activities for M01-M12 and M13-M24).
Keywords:	Dissemination, Training, Standardisation, Exploitation

Editor

Stelvio Cimato (UMIL),

Marion Habernig, Mario Münzer (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	Università 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 third year of the PRACTICE project, providing also a picture of the overall related activities executed over the duration of the 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, during the three years is proved by a good 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.

This deliverable reports also on other dissemination activities supported by the deployment of common dissemination channels, such as the project website, a blog, Twitter account, the participation to social networks, used to further extend the knowledge about the project's activities in both scientific and professional communities.

Furthermore, we report in this deliverable on the exploitation activities undertaken by the project partners individually and in collaboration with other partners, including some successful experiences, as well as some benefits, that the partners collected within the participation in the consortium. Many of the software components and solutions developed in the project (see Figure 6) have a large potential commercial value and are ready to be used in future software solutions or as stepping stones for research and business collaboration, providing a platform for continuous exploitation beyond the duration of the project.

To summarize, the achievements and work towards the project goals during the third project year for dissemination and standardisation include: 19 peer-reviewed scientific publications, 27 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.

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 and D32.2. 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 third year and discusses the achieved targets after monitoring of the activities. Furthermore, we report on the overall activities that have been executed during the whole duration of the project.

1.1 Overall dissemination strategy and evaluation criteria

As already explained in D32.1 and D32.2, 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 1.2.4.1)

Audience	Channels
Scientific communities	scientific publications, academic events, conferences and workshop
Commercial and industry experts	Events, fairs, etc.
General public.	Website, blogs, social networks, newsletters, etc.

Table 1: Target audience and dissemination channel

As reported in Table 1: Target audience and dissemination channel, the audience has been classified into three broad categories and different channels have been selected to disseminate the project results according to the dissemination strategy. For targeting the scientific community, scientific publications and presence in academic events or conferences have been selected. To attract the interest and interact with the eventual beneficiaries of the PRACTICE technology, organization of and participation to events and other related outreach activities have been selected. Finally, the website and other communication means such as blogs, social networks (Twitter, LinkedIn, etc.) newsletters have been used to reach the general public and disseminate the produced materials easily accessible from different channels.

As discussed in the previous version of this deliverable, 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 could be easily detected and appropriate countermeasures undertaken. Once the KPI have been measured, every activity has been evaluated in order to assess if both the dissemination plan was achieving the fixed goals and if the indicators themselves were appropriate for the measurement. The selected KPIs are listed in Table 6: Key performance indicators for the dissemination activities, while a detailed discussion of each dissemination activity and the associated KPIs is contained at the end of this chapter.

1.2 Dissemination activities started in M25-M36

The project and its results have been disseminated by invited talks at conferences, by publications at scientific and industry oriented conferences (such as AvonCrypt, DATE, Eurocrypt, ACNS, ACM CCS 2016, 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 third PRACTICE project year. All scientific publications are listed in an action overview list and are updated by the partners on a regular basis. Currently *19 peer-reviewed scientific publications* were prepared during the third project year. Altogether *64 publications* have been created since project start (M01-M36).

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Number of citations	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Two working titles: "Encrypted Data and the GDPR" and "Joint Controllership"	Gerald Spindler, Philipp Schmechel, Jan Lundberg				2016	NA	NA		
Confidential Benchmarking based on Multiparty Computation	Ivan Damgård, Kasper Damgård, Kurt Nielsen, Peter Sebastian Nordholt, Tomas Toft	Financial Cryptography and Data Security 2016	Springer	Barbados	2016	Events in Cooperation with IACR	6	https://eprint.iacr.org/2015/1006	Yes
Valiant's Universal Circuit is Practical	Ágnes Kiss, Thomas Schneider	Eurocrypt 2016	Springer	Vienna (Austria)	2016	Accepted at one of the top conference in security and privacy, with acceptance rate 23%.	5	http://eprint.iacr.org/2016/093	Yes
Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT	Ágnes Kiss, Juliane Krämer, Pablo Rauzy and Jean-Pierre Seifert	Constructive Side-Channel Analysis and Secure Design (COSADE)	Springer	Graz, Austria	2016	NA	2	http://eprint.iacr.org/2016/238	Yes

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

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

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Number of citations	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
GarbledCPU: A MIPS processor for secure computation in hardware	Ebrahim M. Songhori, Shaza Zeitouni, Ghada Dessouky, Thomas Schneider, Ahmad-Reza Sadeghi, and Farinaz Koushanfar	Design Automation Conference (DAC'16)	ACM	Austin, USA	2016	NA	NA	http://dx.doi.org/10.1145/2897937.2898027	Yes
More Efficient Oblivious Transfer Extensions	Gilad Asharov, Yehuda Lindell, Thomas Schneider, Michael Zohner	Journal of Cryptology	Springer		2016	NA	25		Yes
Towards Securing Internet eXchange Points Against Curious onlooKers (Short Paper)	Marco Chiesa, Daniel Demmler, Marco Canini, Michael Schapira, and Thomas Schneider	Applied Networking Research Workshop (ANRW'16)	ACM	Berlin, Germany	2016	NA	2	https://irtf.org/anrw/2016/anrw16-final5.pdf	Yes
Die neue EU-Datenschutz-Grundverordnung	Prof. Dr. Gerald Spindler	Der Betrieb (DB)	Handelsblatt Fachmedien GmbH		2016	NA	NA		No
Verbandsklagen und Datenschutz – das neue Verbandsklagerecht - Neuregelungen und Probleme	Prof. Dr. Gerald Spindler	Zeitschrift für Datenschutzrecht (ZD)	C.H.BECK oHG		2016	NA	NA		No
A modular treatment of cryptographic APIs: The Symmetric Key case	T. Shrimpton, M. Stam, B. Warinschi	Proceedings of Crypto 2016	Springer	California, (USA)	2016	Accepted at one of the top conference in security and privacy	NA	https://eprint.iacr.org/2016/586	
Foundations of hardware based attested computation and applications to SGX	M. Barbosa, B. Portela, G. Scerri, B. Warinschi	Proceeings of European Symposium on Security and Privacy 2016	IEEE	Saarbrücken, Germany	2016	Accepted at one of the top conference in security and privacy	2	https://eprint.iacr.org/2016/014	

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Impact of publication	Number of citations	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Secure Software Licensing: Models, Constructions, and Proofs	S. Costea, B. warinschi	Proceedings of Computer Security Foundations 2016	IEEE	Lisbon, Portugal	2016	Accepted at one of the top conference in security and privacy	NA		
On the Hardness of Proving CCA-Security of Signed ElGamal	D.Bernhard, M. Fischlin, B. Warinschi	PKC'16	Springer	Taipei, Taiwan.	2016	NA	2	https://eprint.iacr.org/2015/649	
Toward practical secure stable matching	M. Sadegh Riazi, E. M. Songhori, A.-R. Sadeghi, T. Schneider, F. Koushanfar	PoPETs'17	De Gruyter Open	Minneapolis, MN, USA	2017	NA	NA		Yes
Privacy-preserving tax fraud detection in the cloud with realistic data volumes	Dan Bogdanov, Marko Jõemets, Sander Siim, Meril Vaht	Cybernetica Research Reports	Cyber-netica	Tallinn, Estonia	2016	NA	NA		Yes
Implementation and Evaluation of an Algorithm for Cryptographically Private Principal Component Analysis on Genomic Data	Dan Bogdanov, Liina Kamm, Sven Laur and Ville Sokk	3rd International Workshop on Genome Privacy and Security (GenoPri'16)	IEEE	Chicago, IL, USA	2016	NA	NA		
Personal Data and Encryption in the European General Data Protection Regulation	Gerald Spindler, Philipp Schmechel	Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)	Open Access Journal	Germany	2016	NA	NA	urn:nbn:de:0009-29-44408	Yes
Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation	Berry Schoenmakers, Meilof Veeningen, Niels de Vreede	Applied Cryptography and Network Security (ACNS)	Springer	London, UK	2016	NA	NA	dx.doi.org/10.1007/978-3-319-39555-5_19	Yes
Certificate Validation in Secure Computation and Its Use in Verifiable Linear Programming	Sebastiaan de Hoogh, Berry Schoenmakers, Meilof Veeningen	AFRICACRYPT	Springer	Fes, Morocco	2016	NA	1	dx.doi.org/10.1007/978-3-319-31517-1_14	Yes

Table 2: List of publications

1.2.2 Presentations, conferences and workshops

All Presentations, Conferences, Workshops and other dissemination activities are listed in an action overview list and are updated by the partners on a regular basis. Currently the PRACTICE partners participated in 37 events including presentations, conferences and workshops during the third 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	UWUERZ	INFORMS Annual Conference	1-4	11	2015	Philadelphia, USA	>5000	Presentation of paper regarding flexible capacity management with advanced information obtained through supply chain collaboration	International
Conference	Arcelik	ECFI 2015 – 3rd European Conference on the Future Internet	4-7	11	2015	Hamburg, Germany	600	The biggest event for thee Future Internet technologies covering cloud, big data, IoT, M2M and other active research topics. Participants from start-ups to large industry, regional and local stakeholders, municipalities, researchers, government representatives and FI-PPP accelerator projects. Ar	International
Conference	UNIVBRIS	AvonCrypt	10	11	2015	Bristol, UK	-	Partner UNIVBRIS participated to the conference. The main topic was "Computing on Encrypted Data".	International
Web	ALX	Effektivitet.dk	01	12	2015	Denmark	NA	A short article in a Danish business magazine about Secure Computation a various usecases related to PRACTICE, can be found at http://www.effektivitet.dk/magasin/nr-4-2015-risikostyring-i-global-supply-chain.aspx	National
Conference	Arcelik	Innovation Week Istanbul	3-5	12	2015	Istanbul, Turkey	60,000	The biggest innovation Event in Turkey over 60 thousand participants mainly from Turkey but including many international speakers and partner countries from Europe.	National
Workshop	BIU	6th Bar-Ilan Winter School on Cryptography - Cryptography in the Cloud - Verifiable Computation and Special Encryption	4-7	1	2016	Ramat Gan / Israel	N/A	The topics are verifiable computation and different types of encryption methods that enable clients to encrypt data and carry out limited processing (e.g., search) while keeping it encrypted.	International
Conference	ALX	Financial Cryptography and Data Security 2016	22-26	2	2016	Rockley, Barbados	100	Presenting a paper on work done in WP23, titled "Confidential Benchmarking based on Multiparty Computation"	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				
Workshop	INTEL	Dagstuhl Workshop on Smart Grid Security	18-20	1	2016	Dagstuhl / Germany	20	Discussion on enhancing privacy using secure multi-party computation.	International
Other	TEC, ALL partners	PRACTICE Newsletter Issue 3		2	2016	Online	N/A	Newsletter can be downloaded from PRACTICE website https://practice-project.eu/downloads/publications/newsletter/PRACTICE-Newsletter-Issue4-Feb2016.pdf	International
Conference	INTEL	DATE 2016 Conference	15-18	3	2016	Dresden, Germany	400	Hardware design conference in Europe. Organized a special day on secure systems	International
Conference	CYBER	Estonian Cloud Computing Conference	8	3	2016	Tallinn, Estonia	50	Presentation of secure computing capabilities, including PRACTICE fraud detection prototype.	National
Conference	ARC	Innovation Week Izmir	17-18	3	2016	Izmir, Turkey	9000	Arçelik is the main sponsor of the event. Over 9 thousand participants mainly from Turkey but including many international speakers and partner countries from Europe. Arçelik presentation about innovative projects including PRACTICE and distribution of PRACTICE broschure at the Arçelik stands in the exhibition areas.	International
Symposium	INESC TEC	COST CryptoAction	6-8	4	2016	Budapest, Hungary	100	Annual event of the COST Action on Cryptography, where the work developed by INESC in PRACTICE has been presented, namely that centering on the use of Intel's SGX for outsourcing computations.	International
Conference	ARC	Innovation Week Ankara	4-5	5	2016	Ankara, Turkey	7000	Over 7 thousand participants mainly from Turkey but including many international speakers and partner countries from Europe. Arçelik is the main sponsor of the event. PRACTICE project broschures are distributed at the Arçelik stands in the exhibition areas.	International
Conference	ARC	Industrial Technologies 2016 Amsterdam	22-24	6	2016	Amsterdam, The Netherlands	1200	The largest networking conference in the field of new production technologies, materials, nanotechnology, biotechnology and digitalisation in Europe, with high level delegates. PRACTICE brochures were distributed to the participants at the related sessions during the event.	International
Summit	ARC	Arçelik Global Suppliers Summit	25	5	2016	Istanbul, Turkey	~1000	Arçelik Global Suppliers Summit was held in WoW Istanbul Hotel and around 1000 representatives of Arçelik suppliers were participated at the event. PRACTICE poster has been shown at the exhibitin area and brochures were distributed to the interested parties.	International
Presentation	UWUERZ	Presentation of project results at Alfred Kärcher GmbH & Co. KG	18	2	2016	Winnenden, Germany	20	Presentation of PRACTICE results in meeting regarding discussion of potential collaborative projects.	National

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				
Presentation	TUDA	Eurocrypt 2016	11	5	2016	Vienna, Austria	~300	TUDA presents PRACTICE results at a conference	International
Presentation	TUDA	MPC Workshop 2016	2	6	2016	Aarhus / Denmark	~100	TUDA presents PRACTICE results at a conference	International
Presentation	TUDA	Estonian Winter School in Computer Science (EWSCS) 2016	28-29 1-4	2 3	2016	Palmse, Estonia	~50	TUDA gives lecture series on PRACTICE results with title "Practical secure two-party computation and applications"	International
Workshop	SAP	Dagstuhl Seminar 16051 "Modern Cryptography and Security: An Inter-Community Dialogue"	31-2	1	2016	Dagstuhl, Germany	20	Presentation and discussion of PRACTICE results	International
Workshop	SAP	Financial Crypto Anniversary panel	18-29	2	2016	Rockley, Barbados	100	Presentation and discussion about “The Promise and Pitfalls of Distributed Consensus Systems: From Contract Signing to Cryptocurrencies"	International
Workshop	SAP	Summer School on Secure and Oblivious Computation and Outsourcing	9-11	5	2016	Notre Dame, Illinois	~15	Summer school where recent PRACTICE results have been discussed	
Exhibition	DTA, CCII-UNISA	Taranto-Grottaglie Test Bed	15	3	2016	Grottaglie, Taranto (IT)	100	presentation of the Grottaglie Airport Test Bed (research infrastructure)	National
Conference	TUE	ACNS 2016	19-22	6	2016	London / UK	100	Present paper on privacy-preserving verifiable computation	International
Workshop	CYBER	DIMACS/MACS Workshop on Cryptography for the RAM Model of Computation	8-10	6	2016	Boston, MA, USA	50	Dan's talk included some results from PRACTICE	
Conference	UNIVBRIS	ACNS	19-22	6	2016	London	100	B. Warinschi gave a keynote talk on the project's results on the use of SGX for trustworthy computation	International
Exhibition	DTA	Farnborough International Airshow	11-12	6	2016	Fornborough (UK)	50	Exhibition of the most recent innovation related to aviation industry, DTA informed on research activities, hosted in the information stand of Regione Puglia	International
Conference	Intel / TUDA	SPMED Workshop on Security and Privacy for Collaborative Medical Analytics	18	7	2016	Darmstadt / Germany	60	Focus on privacy for Secure MPC in medical. Ahmad Sadeghi, Matthias Schunter were co-organizers.	International
School	INESC	CUSO Doctoral School	20	9	2016	Neuchatel, Switzerland	15	Doctoral school, where INESC’s work in PRACTICE was presented to young researchers.	

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	Intel	ACM CCS 2016	26	10	2016	Vienna, Austria	300	Presentation of PRACTICE results in meeting regarding discussion of potential collaborative projects.	International
Conference	UNISAlento/ DTA	Collaborative Supply Chain and Data Protection	05	10	2016	Bari, Italy	20	presenting the methodology for data protection in collaboraitve business models and the PRACTICE fleet management case	National
Presentation	UNISAlento/ DTA	Collaborare e competere: gestire il rischio di perdita di dati confidenziali	17	10	2016	Lecce, Italy	150	presenting the methodology for data protection in collaboraitve business models and the PRACTICE fleet management case	National
Presentation	UMIL	Controlling Leakage and Disclosure Risk in Big Data applications	30	9	2016	Heraclion-Crete, Greece	~200	extending the PRACTICE approach: to a quantitative technique for computing Big Data leakage risk estimates	International
Conference	ARC	5. R&D Centres Summit	27-28	9	2016	Ankara, Turkey	4000	Arçelik has won the most innovative R&D Centre award at the event. PRACTICE is included among the exhibited Arçelik projects in the Arçelik stand at the exhibition area. PRACTICE project info is shared and brochure is distributed to the interested visitors at the Arçelik stand in the exhibition area.	National
B2B Event	ARC	Industry 4.0 Turkey Brokerage Event	15	7	2016	Bursa,Turkey	120	Industry 4.0 Turkey Brokerage Event offered business contacts to industry, science and nanotechnology professionals who were looking for potential partners in Turkey and other countries to ensure sustainable business development and growth. PRACTICE project was mentioned in Arçelik presentation and brochures were distributed to the participants during the event.	International
Conference	ARC	Innovation Week Adana	27-28	10	2016	Adana, Turkey	3000	Arçelik is the main sponsor of the event. Arçelik has included PRACTICE among the innovative projects presentation. PRACTICE brochure is distributed at the Arçelik stands in the exhibition areas.	International

Table 3: Presentations, conferences and workshops

1.2.3 PRACTICE project website statistics

In the following, we present statistics generated from the PRACTICE project website (www.practice-project.eu) to underline the successful dissemination activities.

1.2.3.1 Website visitors

A statistical analysis of access (both unique visitors and overall visits) to the PRACTICE project website for a 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 last project period from the 1st of November 2015 to the end of October 2016.

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.

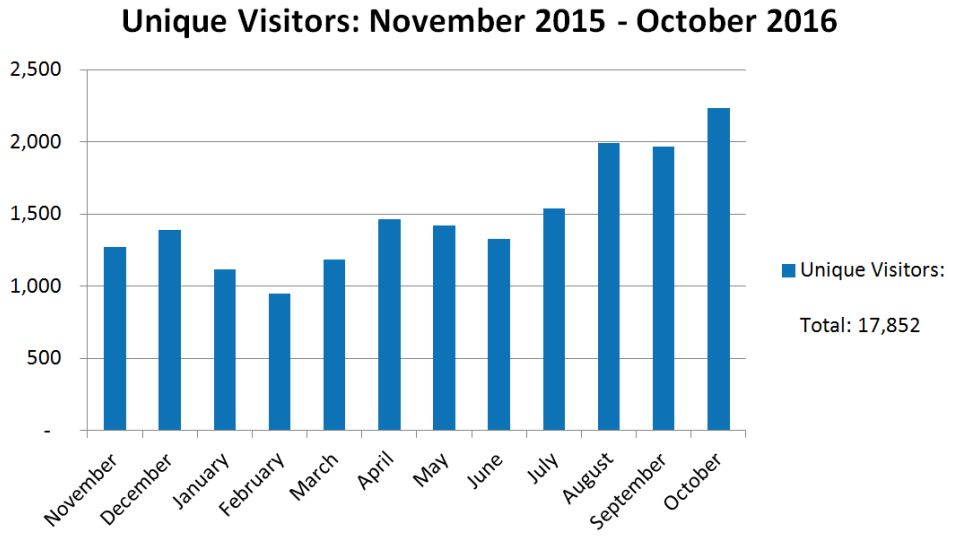

Figure 1: PRACTICE website statistic of unique visitors

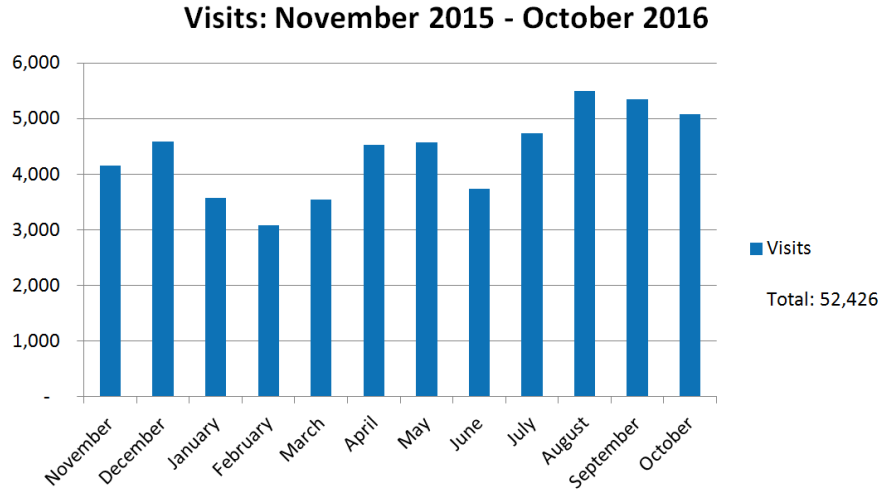

Figure 2: PRACTICE website statistic of non-unique visits

During the third project period the PRACTICE website has been visited 52.426 times in total by 17.852 unique visitors. These numbers reflect the growing popularity of the PRACTICE project. In year two, the website was visited 47,073 times by 13,943 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 quarter is represented by Asia. The remaining percentage is spread over America, 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.

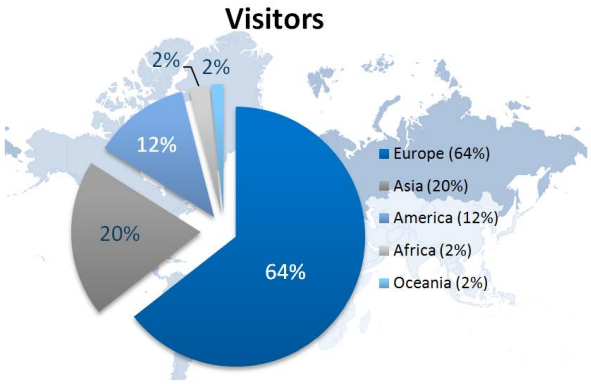

Figure 3: PRACTICE website statistic of the geographical distribution of visitor's location

With respect to the following statistic (Figure 4), it has to be pointed out that in the third project period of PRACTICE, the website has been able to attract a considerable amount of new visitors, representing more than 79% of the overall visitors.

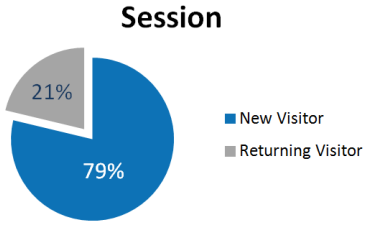

Figure 4: PRACTICE website statistic of the distribution of the type of the visitors

Considering the top downloaded documents during the third project period, the deliverable D21.2 "*Unified architecture for programmable secure computations*" was the most frequently viewed/downloaded document of the PRACTICE website, as shown in Figure 5. Since the publication of the fourth issue of the PRACTICE newsletter in February 2016 this document was downloaded 1,177 times, being the second most viewed PRACTICE document. This is followed by D31.3 "*Risk assessment and current legal status on data protection*" with 1,174 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 Cryptoprocessor*" prove notable hits.

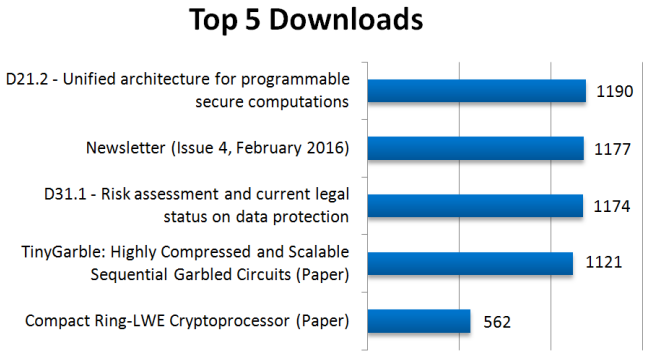

Figure 5: PRACTICE website statistic of the most frequently viewed/downloaded documents

1.2.3.2 Website Maintenance/Eventual Out-phasing

The website will be maintained for three years after the project (i.e. 2017-2020). Afterwards some project information will be available on the website from TEC (http://technikon.com/). Long-term storage of project results previously not stored elsewhere (e.g. public deliverables) has been addressed by their additional submission at zenodo.org. Zenodo is a repository for scientific publication and data hosted by CERN, supported by the European Union.

1.2.3.3 Project newsletters

The newsletters offer current information and disseminate important events. The newsletters can be found on the PRACTICE website and are also posted via the PRACTICE Twitter and LinkedIn account to catch further public awareness. The 4th newsletter was issued in February 2016 and the final and fifth newsletter will be issued in October/November 2016. Table 4 reports the number of downloads for each item released during the project's duration.

Document	Downloads
Newsletter (Issue 1, March 2014)	269
Newsletter (Issue 2, July 2014)	294
Newsletter (Issue 3, March 2015)	552
Newsletter (Issue 4, February 2016)	1177
Announcement-Letter	307
Poster	343
Roll-Up	221
Leaflet	237

Table 4: 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. Therefore, 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". The PRACTICE project is available on https://twitter.com/FP7_PRACTICE.

Since M25 there have been 79 tweets in total – as planned 1-2 tweets per month. Currently the PRACTICE consortium has 80 followers as reported in Table 5.

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 58 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

Social Network	#
Twitter	79 tweets (+46) 5 tweets and 33 retweets within this project period 80 follower (+37)
LinkedIn	58 members (+3)
Blog	17 entries 3 entries within this project period

Table 5: Number of contacts for social networks

1.2.4.1 Cooperation with other projects

The cooperation activities reported in D32.1 and D32.2 have been fostered during the third year of the project. PRACTICE continued with providing latest information, newsletters etc. to the related projects that are listed on the official website: http://www.practice-project.eu/links. Interesting material that has been received from the related projects has been distributed within the PRACTICE consortium as well. Further the cooperation with the Tartu city government has been fostered as well as the cooperation between the H2020 projects SUPERCLOUD and SafeCloud where PRACTICE partners participated in the kick-off meeting in October 2015.

1.2.5 Analysis of the dissemination activities

A number of KPI have been selected in order to monitor the dissemination activities and take appropriate countermeasures in case of deviations from the fixed goals. Periodic measurements w.r.t. those indicators of each activity have been taken in order to assess if both the dissemination plan was needing corrections and if the indicators themselves were appropriate for the measurement. The selected KPIs are listed in Table 6,

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 6: Key performance indicators for the dissemination activities

The overall judgment about the activities during the third year is positive, since all the KPIs have been satisfied. In the following the individual dissemination activities are analysed in detail.

1.2.5.1 Scientific Conferences and Journals.

About the publications of papers in international journals and proceedings of workshops and conferences, the thresholds have been overcome in the third year. In Table 2, 19 publications have been reported targeting the most important journals and scientific events in the area, involving a large number of attendees in case of conferences. This numbers assess also the quality of the work done in PRACTICE, since the events are listed as the ones with the largest impact factor in the scientific community. So the threshold for the KPI regarding "**Impact factor**" for conferences (at least 2 papers out of 11 foreseen publications in the top 20 conferences) has been overcome also in 2016.

The dissemination activities performed during the third year, satisfy the KPIs achieving successful results both for quality and quantity of the scientific publications.

1.2.5.2 Presentation/Workshops

As reported in Table 3, project's partners have increased also the commercial dissemination activities, organizing and participating to presentations involving a large number of attendees. KPIs related to "Number of events" and "Number of attendees" have been abundantly overcome, extending the outreach of the project activities also countries outside of Europe.

1.2.5.3 Website

Numbers reported in section 1.2.3, about the visits received during the third project period, (52.426 visits in total by 17.852 unique visitors) confirm the growing popularity of the PRACTICE project and a successful strategy. Both indicators that have been selected as KPIs, "Number of visits" and "Number of unique visitors", 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.

1.2.5.4 Newsletters/Fact Sheets/Posters

Table 4 reports the number of downloads for each item released during the project's duration. Also in this case KPI have been satisfied for all of the considered dissemination activities, resulting in a large number of contacts and people interested in the project activities.

1.2.5.5 Social Networks/Blogs

Also using social networks to spread project information has been successful, since the number of followers has doubled and the activities have been advertised with an adequate number of posts using the blog and the restricted group of interested people.

Chapter 2 Standardisation strategy in M25-M36

Our focus continued to be the creation of a market for PRACTICE technologies. Standardisation makes technologies feel more mature and can improve adoption in more conservative markets that can otherwise be the perfect users for secure computing technology.

In Year 3, we planned to continue working on fundamental cryptography standards (secret sharing, homomorphic cryptography), but also encourage the use of cryptographic technologies in privacy.

2.1 Standardisation results in M25-M36

The consortium prepared comments for ISO/IEC JTC 1 SC 27 (Information security technologies) meetings. We wrote two rounds of comments.

First, for the Tampa meeting in April 2016 in the United States of America, we prepared two sets of comments.

1) ISO/IEC 18033-6 Encryption algorithms — Part 6: Homomorphic encryption. 7 comments, 1 accepted, 6 requiring further input from National Bodies.
2) ISO/IEC 20889 Privacy-enhancing data de-identification techniques. 10 comments + annex proposed, all material accepted.

For the Abu Dhabi meeting in October 2016 in the United Arab Emirates, we prepared one set of comments.

1) ISO/IEC 20889 Privacy-enhancing data de-identification techniques. 15 comments. Response not received by the time of preparing this report.

In the World-Wide Web Consortium (W3C), partner INTEL continued to chair the Tracking Protection Working Group (TPWG). The goal of this working group is to allow users to express a preference not to be tracked and to enable web-sites to explain their traffic behaviour to end users. In M25-M36 we reached multiple important milestones:

- Candidate Recommendation of Tracking Preference Expression (TPE): The TPE standard was published as candidate recommendation. This is the last state before becoming a standard. We are currently gathering implementation feedback to then progress into a Final Recommendation.
- Candidate Recommendation of Tracking Compliance Specification (TCS): The TCS standard defines how websites can comply. It also matured into Candidate Recommendation state and waits adoption.

2.2 Per-partner standardisation report for M01-M36

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

As coordinator, **TEC** actively supported the standardisation activities of the consortium and provided assistance where needed and appropriate. Furthermore TEC was the interface between the Standardisation Institute and the partners.

CYBER was responsible for maintaining the liaison with ISO/IEC JTC 1 SC 27 working groups 2 and 5 and preparing comments to standards 18033-6, 19592-1, 19592-2, 20889 and 29151. To summarize the impact of this work, we give a status of these standard.

ISO/IEC 18033-6 Encryption algorithms — Part 6: Homomorphic encryption – standard still under development, PRACTICE technologies are included in the draft.

ISO/IEC 19592-1 Secret Sharing – Part 1: General – standard completed and will be published in 2016, PRACTICE technologies are included in the final version.

ISO/IEC 19592-2 Secret Sharing – Part 2: Fundamental mechanisms – standard in its final stages, expected to be completed in 2017, PRACTICE technologies are included in the final version.

ISO/IEC 20889 Privacy-enhancing data de-identification techniques – standard under development, PRACTICE technologies are included in the draft.

ISO/IEC 29151 Code of Practice for PII Protection – standard being completed, guidance includes suggestions to consider technologies like the ones proposed in PRACTICE.

INTEL focused on increasing demand for cloud privacy by chairing and contributing to the W3C Tracking Protection Working Group.

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 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. The RACS workshop aims to present a comprehensive overview on regulatory and standardization 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.

In 2015 the Workshop had finalized its first deliverable (https://www.cen.eu/work/areas/ICT/eBusiness/Pages/WS-RACS.aspx) 'RACS - Requirements and Recommendations for Assurance in Cloud Security — Part 1: Contributed recommendations from European projects' which consists of a set of recommendations on security assurance management in the context of auditing and certification of cloud-based services and systems.

In 2016, CEN workshop RACS, under the chairmanship of Ernesto Damiani (https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:1214399&cs=106839FD3EAB76EDA2284241D8F3194D2) has continued the preparation of its second CWA on certified cloud security controls based on the current audit frameworks.

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, the individual updated exploitation plans in section 3.3, and joint exploitation activities in section 3.4.

3.2 Exploitation success 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

SAP has grown to become the world's leading provider of business software solutions. With 12 million users, 96,400 installations, and more than 1,500 partners, SAP is the world's largest enterprise software company and the world's third-largest independent software supplier, overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP industry solutions support the unique business processes of more than 25 industry segments, including high tech, retail, manufacturing and financial services.

Bill McDermott, CEO of SAP, has recently announced at the New York stock exchange S4/HANA as its new core product replacing ERP. This move puts the HANA platform at the center of the SAP product portfolio. Furthermore it enables products to be seamlessly deployed on-premise, in the cloud or as a hybrid. This puts security even more into the focus and the security department of SAP, including its research division, consults development in order to ensure safe and secure software services and products. It is placed under Bernd Leukert's software development organization and hence the development groups are our main stakeholders for transferring and exploiting the research results.

Started in 2012, SAP Security Research has paved the way for novel services providing security for SAP's customers by starting 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 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. Problems crucial in deployment, such as integration or on-boarding, are often overlooked in scientific research. SAP’s research team invented and implemented a number of ground-breaking approaches and extensions in this area.

In recent years, the SEEED project gathered significant internal attention within SAP. Several discussions with stakeholders – including the top executive level – took place. The team was 1st runner-up within the development organization for the prestigious internal Hasso Plattner’s Founders Award. Following initial discussions, teams – including product groups, central security and security research – were formed to transfer SEEED to the product roadmap. Following an internal alignment process – including again top-level executives – this roadmap was finalized.

Inspired by the research results of SEEED enabled by PRACTICE, SAP and its internal development group are working on a data management system for HANA which supports encryption: adopting essential concepts of SEEED, single columns of a database can be encrypted with a randomized or deterministic encryption scheme. This allows equality searches over encrypted data. Range queries or aggregations are not yet supported but might be published in the future, following the methodology developed, enhanced and evaluated during PRACTICE. SAP aims at offering a complete cloud transition lifecycle solution that covers (1) analysis of data structures before outsourcing them, (2) outsourcing of data into the HANA Enterprise Cloud Infrastructure respecting data ownership principles, as well as (3) support for an encrypted, searchable database on basis of HANA.

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 H2020 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 including 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 is an application that is easy to relate to and ideal as show-case of the technology. Also, the fact that the survey system can run on both Sharemind and Fresco/SPDZ is an important signal to end users, e,g, by addressing the risk of being too locked into service providers. It furthermore functions as a common ground for future collaboration and joint exploitation beyond PRACTICE between the partners in WP23 CYBER, ALX and PAR.

The developed confidential benchmarking application has involved many end users and business partners e.g. several banks, a consultancy house and other financial organisations. The application is general and has been used to sell the idea of using MPC in financial risk assessment and statistics more generally.

Finally, the combined use of the survey and the benchmarking application has lead to important improvements in both systems and illustrates more broadly the field of use. Also, it strengthen our ability to show case the value of secure statistics, needed to convince end users, business collaborators and investors.

The above activities on secure statistics in PRACTICE has opened up for new exploitation opportunities, further supported by the spinout project “Big Data by Security” supported by the Danish industry foundation. This project involves two practical applications that built on the results from PRACTICE and involve more end users. The first case involves banks and a P2P crowd-lending site, and MPC will be used to include more confidential information in credit rating and enhance the competition on loans. The second case involves Statistics Denmark directly, and aims at making sensitive data available for tailored collaborative statistics outside of Statistics Denmark using MPC. In parallel, PAR is negotiating with business partners about the foundation for a future spinout with Secure Statistics as it’s focal point. As in the case of Sepior, this process is an opportunity to set the right team and focus to make the spinout suiitable for end users, business partners and investors. The PRACTICE project has been instrumental and a direct stepping stone for this development.

3.2.3 CYBER

In the third year of the project, Cybernetica significantly extended its exploitation activities. These efforts directly build on the previous work done in the project.

First, Cybernetica included the tax fraud detection story in its direct marketing materials and has since then conducted a first commercial pilot with a European customer. Due to confidentiality agreements, it is currently impossible to disclose details, but Cybernetica was able to deliver a commercial prototype by significantly rewriting the PRACTICE research prototype to be more resilient and capable. We also evaluated this commercial prototype in a public cloud environment to great results – the costs were acceptable for the customer. We are now pursuing options to turn this pilot project into a full commercial contract.

Second, enabled by the reallocation of PRACTICE efforts, CYBER extended the survey system to support large real-world surveys and then organised the employee satisfaction study at the Tartu city government. Although the study was supposed to run in 2015, additional engineering work and delays with the customer postponed the study to 2016. However, it was conducted successfully and the customer is planning future studies as well. Given that more than ten studies (most of them smaller) have been run with the PRACTICE cloud-based survey system, we will certainly be looking for ways to bring this capability to the market with our partners who have also invested efforts in it.

Third, CYBER has started looking for exploitation opportunities in the medical field. By participating at the iDASH Genomic Privacy challenge we hope to gain additional visibility for the genomic privacy work done in PRACTICE. CYBER is approaching European biotech companies with the offering of privacy-preserving data exchange. While no commercial contracts have been signed yet, we are hoping to sign the first customers in 2017.

Finally, the PRACTICE SDK effort driven by CYBER has been significantly expanded with the integration of the cloud deployment service developed in PRACTICE. Designed following

the feedback from the advisory board, the deployment system will simplify the process of using PRACTICE technologies. Again, we hope to sign the first customers in 2017 and we are also looking for ways to integrate the created capability with governmental cloud platforms, e.g., G-Cloud and the Estonian government cloud. For the latter, Cybernetica is also in the consortium that won the tender to build and deploy governmental cloud services and CYBER is also responsible for data security policies.

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 3rd project year	**TEC** further worked in the field of secure computation and enhanced its recently developed secure survey ("Doodle") application prototype. The so-called *Doodle* enables privacy-preserving participation on a survey/poll by means of Fully Homomorphic Encryption (FHE) Scheme, a technology described within PRACTICE, which allows operations on ciphertexts without a prior-encryption of each vote. TEC expand the prototype by its answer options: while the first prototype was able to make use of only the answers yes and no, respectively 1 and 0, the enhanced version is able to perform computations on multiple answer options. In order to reduce the computational effort on the application servers, sophisticated computations were outsourced to the cloud. However, the outsourcing of computational effort to the cloud is uncritical, since the provided data is encrypted and useless without the corresponding key. The cloud is performing calculations directly on the ciphertexts. As a result of this, the cloud is providing the coordinator with survey results in a still encrypted and privacy-preserved way. TEC were still able to enhance its knowledge during the 3rd year in security & privacy of cloud applications. 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 3rd 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 exploitation activities after 3rd project year	In the final year the plan was to initiate the technology transfer of our developed cloud encryption solution into development teams. Therefore, we continued our efforts and held meetings with several potential customers as well as internal stakeholders in product development with focus on actual technology transfer into their products. In total, our results regarding the exploitation for PRACTICE are as follows: • Adopting essential concepts of SEEED enabled by PRACTICE, SAP and its internal development group are working on a data management system which supports encryption while providing equality searches on this encrypted data. We held successive meetings with various internal stakeholder I In the final year the plan was to initiate the technology transfer of our developed cloud encryption solution into development teams. Therefore, we continued our

Partner 2: SAP AG (SAP) – Germany	
	efforts and held meetings with several potential customers as well as internal stakeholders in product development with focus on actual technology transfer into their products. In total, our results regarding the exploitation for PRACTICE are as follows: • Adopting essential concepts of SEEED enabled by PRACTICE, SAP and its internal development group are working on a data management system which supports encryption while providing equality searches on this encrypted data. • We held successive meetings with various internal stakeholder groups and agreed on a follow-up with the SAP HANA product management. • We presented at a highly coveted spot at SAP DKOM in Palo Alto to the entire product development organization. • At SAP TechEd in Las Vegas, Justin Somaini, Chief Security Officer of SAP, identified Zero Knowledge Systems, including the SEEED technology developed within the PRACTICE Project as one business enabler for SAP's future. • On a detailed system architecture basis, we developed a comprehensive transfer roadmap for one specific internal stakeholder and initiated the legal processes for software export
Updated exploitation plan after 3rd project year including stakeholder	In its half-year report, **SAP** has reported a proceeding of the growth in the cloud market – the revenue of cloud subscriptions and support has increased by 32% (to € millions: 1,397). As announced by Bill McDermott, CEO of SAP, "Our groundbreaking new architecture is accelerating momentum across all businesses". This statement combined with the efforts of SAP's Chief Security Officer Justin Somaini, to push Zero Knowledge Systems as a business enabler consequently puts security into the strategic focus of SAP. As a result, we expect secure cloud applications and encrypted databases as key elements for SAP's continuous growth in the cloud. Therefore, we will continue our efforts and contact additional internal product groups as well as external customers. Furthermore, our goal is to support them with knowledge gained during this project as well as distribute source code and architectural documents developed within the last three years driven by PRACTICE. In addition, our goal is to improve further aspects of the SEEED project in follow-up Horizon2020 Projects ESCUDO-CLOUD and TREDISEC.

Partner 3: Technische Universitaet Darmstadt, Intel Collaborative Research Institute for Secure Computing (TUDA) – Germany	
Report on exploitation activities after 3rd project year	In the third year, **TUDA** published several research papers at conferences (EUROCRYPT'16, DAC'16, ANRW'16, PETs'17) and scientific journals (Journal of Cryptology). We further improved and extended the list of our prototype implementations that were available at http://encrypto.de/code. Thomas Schneider from TUDA gave a lecture series at the 21st Estonian Winter School in Computer Science (EWSCS), in Palmse, Estonia, February 28 - March 4, 2016 on "Practical secure two-party computation and applications". Besides this, Michael Zohner from TUDA gave a presentation on Efficient OT Extension and its Impact on Secure Computation at the Theory and Practice of Secure Multiparty Computation Workshop in Aarhus, Denmark, June 3, 2016. In the winter term 2015/16 we offered a seminar on "privacy-preserving technologies" at TUDA, in which students could get to know several PRACTICE results developed in the project. The seminar received excellent feedback from the participants, who had to comprehend, summarize and

Partner 3: Technische Universitaet Darmstadt, Intel Collaborative Research Institute for Secure Computing (TUDA) – Germany	
	present two research papers in the area of secure multiparty computation, with a main focus on applications. Several students continued showing interest in the field and continued working on their selected topics, e.g. in 4 Bachelor theses.
Updated exploitation plan after 3rd project year including stakeholder	We will continue focusing on showing the practicality of secure computation technologies by means of top publications and prototype implementations. In the current winter term 2016/17 we are offering the seminar "privacy-preserving technologies" again. Besides, TUDA will continue working on secure computation technologies as part of successor projects.

Partner 4: Alexandra Institutte A/S (ALX) – Denmark	
Report on exploitation activities after 3rd project year	In the third year of PRACTICE, **ALX** has worked on improving all of the software mentioned in the second year reports, including the FRESCO framework, and has delivered the financial benchmarking prototype and the deployment tool. Additionally, we have implemented a new secure computation protocol developed by researchers at Aarhus University.
Updated exploitation plan after 3rd project year including stakeholder	Updated exploitation plan after 3rd project year including stakeholder: ALX plans to continue many of the efforts we have worked on throughout the PRACTICE project. This includes improving the FRESCO framework for secure computation, and developing new prototypes based on secure computation. This will be done as part of other research projects, including the H2020 project SODA, which will focus on data analytics based on secure computation. Additionally, we will uses the knowledge and skills developed in the PRACTICE project for advising Danish small and medium sized companies in how to utilise secure computation, and to develop commercially viable software solutions for the Danish market.

Partner 5: Arçelik A/S (ARC) – Turkey	
Report on exploitation activities after 3rd project year	**ARC** 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 third year. Arcelik's suppliers has also been informed about the project outcomes and the potential benefits during Arçelik Global Suppliers Summit on the 25th of May in Istanbul. PRACTICE project poster were shown and brochures were distributed at Arcelik stands in a number of events during the third project year including 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 3rd project year including stakeholder	**Arcelik** is planning to present PRACTICE project at the Koc Technology Board event "Technology Day" which is planned on the 4th of November in Istanbul showing potential outcomes and exploitation possibilities to inform Koc Group of companies active in car manufacturing, energy, finance and agri-food sectors. Arcelik is planning to show PRACTICE poster, distribute brochures and show VMI demo at its stand in events, trade shows where Arcelik will participate in the last quarter of 2016 and 2017..

Partner 6: Bar Ilan University (BIU) – Israel	
Report on exploitation activities after 3rd project year	In the 3rd 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.

Partner 6: Bar Ilan University (BIU) – Israel	
	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 3rd project year including stakeholder	In the 3rd year of the project, BIU focused many efforts on further developing the SCAPI software library, based on the observations and conclusions in the first two years of the project. BIU also organized and hosted the 6th BIU winter school, on January 4-7, 2016. The school focused on cryptography in the cloud – verifiable computation and special encryption.

Partner 7: Cybernetica AS (CYBER) – Estonia	
Report on exploitation activities after 3rd project year	In the third year, **CYBER** advanced its exploitation work on all fronts. Most notably, we were able to reach a first commercial contract with a European customer who learned about the research pilots we built in PRACTICE. The success of the jointly developed privacy-preserving cloud-based survey system drove our additional work towards cloud platforms. We took the survey system closer to maturity and built a service that simplifies the development of PRACTICE technologies on the cloud. The latter is also integrated with the PRACTICE SDK and CYBER's commercial offerings around the Sharemind platform. We also started marketing the secure computing capabilities developed for PRACTICE within the genomic privacy space.
Updated exploitation plan after 3rd project year including stakeholder	CYBER plans to exploit the results of the PRACTICE project after the project as follows. 1) We will continue to use the PRACTICE research prototypes and their case studies in our marketing. 2) We are negotiating with ALX and PAR to continue developing the joint cloud-based offerings, with the survey system and its statistical extensions as the first target. 3) We are planning to include more foundational technology from TUDA (CMBC-GC) and BIU (SCAPI) in our platforms where relevant. 4) We are negotiating with INTEL to continue our joint exploration of the privacy-preserving data analysis space. 5) We will continue working with INESC TEC to include their program analysis technology with CYBER's Sharemind platform, the PRACTICE SDK and the PRACTICE cloud deployment system.

Partner 8: Julius-Maximilians Universitaet Wuerzburg (UWUERZ) – Germany	
Report on exploitation activities after 3rd project year	**E**xploitation activities of **UWUERZ** in the 3rd year were focused on three areas: First, we use our contacts with companies that could benefit from PRACTICE results; second, within our teaching activities we raise awareness for PRACTICE ideas amongst the future generation of decision makers; third, with scientific publications and presentations at scientific conferences we spread PRACTICE results within the scientific community in the field of supply chain management and operations research. More specific, we work with the biggest European service provider for maintenance in aerospace industry and raise awareness for potential use cases of cloud based collaboration in maintenance supply chains as developed in work package 2.4. We held a seminar named *Supply Chain Collaboration* that raised awareness for privacy issues and PRACTICE activities. Three additional master's theses related to PRACTICE contents were completed. Members of the **UWUERZ** team present PRACTICE results related to

Partner 8: Julius-Maximilians Universitaet Wuerzburg (UWUERZ) – Germany	
	supply chain management at the *Conference for Data Drive Operations Management*. We published a paper in the *European Journal of Operational Research*. In addition, we submitted a paper on "Secure Supply Chain Collaboration" to a special issue of *Computers and Operations Research*.
Updated exploitation plan after 3rd project year including stakeholder	After the 3rd year, we will focus our exploitation activities on our work with industrial partners. We are in contact with several German small and medium sized companies which are interested in data driven use cases for their operations with high requirements for data security. Here, we promote secure cloud infrastructure as key enabling technology.

Partner 9: Intel GmbH (INTEL) – Germany	
Report on exploitation activities after 3rd 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. Finally we started collaborating with CYBER to provide hardware security underpinning to further add defence in-depth to the CYBER ShareMind system. Our Intel SGX technology allows ShareMind tasks to run in hardware-isolated enclaves.
Updated exploitation plan after 3rd project year including stakeholder	**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 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 3rd project year	In the third year **KU Leuven** has published two papers on side-channel security of ring LWE: one at the Journal of Cryptographic Engineering 2016 and the other at the PQ Crypto 2016 conference paper. A third paper has been accepted at CANS 2016 on MPC privacy-reserving protocol for a local electricity trading market. . All works are directly related to the project.. These results have been further disseminated at seminars, lectures, and industrial events. KU Leuven is in the process of preparing two submissions to the Financial Crypto 2016 conference on the topics of MPC privacy-reserving protocol for smart metering and MPC-based protocol for keyless car sharing system. Another work is prepared for submission to the journal of Transaction on Computers on assisting homomorphic function evaluation and encrypted search operations. KU Leuven has also conducted collaborations with other research institutions from the project network.
Updated exploitation plan after 3rd 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.

Partner 11: INESC PORTO – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC Porto) – Portugal	
Report on exploitation	Collaboration with PRACTICE partners has led to the identification of a use case for verifiable computation in the area of smart metering, which has

Partner 11: INESC PORTO – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC Porto) – Portugal	
activities after 3rd project year	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 project has run its first year in parallel with the third year of PRACTICE. During this year, techniques for securing database technologies have been selected and an architecture for secure databases has been defined that directly rely on techniques and expertise developed in PRACTICE. National project NanoStima has also started in 2016, and one of the central components in the project is an infrastructure for secure data storage and management, that will rely on prototypes and know-how obtained during the PRACTICE project.
Updated exploitation plan after 3rd project year including stakeholder	European projects SafeCloud and LightKone—the latter will begin in 2017---as well as national project NanoStima, will give continuity to INESC Porto's work in PRACTICE for the next three years. INESC Porto will also continue to be actively involved in dissemination of the PRACTICE results via scientific publications, participation in industrial events, and training activities.

Partner 12: Aarhus Universitet (AU) – Denmark	
Report on exploitation activities after 3rd project year	**AU** has published papers at top-tier scientific venues (CRYPTO, EUROCRYPT, TCC, Usenix Security, etc.). In particular, AU researchers won the best student paper award at Usenix 2016. Researchers from AU have been invited to lecture about the research developed in this project at international PhD school (ECRYPT-NET) and to give invited talks at international conferences (INDOCRYPT).
Updated exploitation plan after 3rd project year including stakeholder	The experience maturated in this project has helped AU to attract further funding for continuing our research in the theory and practice of secure multiparty computation, both at a national and at a European level. After the end of the project AU will continue to investigate the theory and practice of MPC technologies, thanks to both national and EU funding.

Partner 13: Technische Universiteit Eindhoven (TUE) – Netherlands	
Report on exploitation activities after 3rd 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. TUE has also submitted a proposal for a follow-up project, which has been granted by the EU: H2020 SODA (Scalable Oblivious Data Analytics) project.
Updated exploitation plan after 3rd 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, CWI). Furthermore, we have broadened our research into secure multiparty computation, extending into several directions all connected to verifiability, resulting in several papers. Finally, we have worked on several prototypes, partly relying on VIFF and SCAPI. All these activities reinforce TUE's position as a center of

Partner 13: Technische Universiteit Eindhoven (TUE) – Netherlands	
	expertise in secure multiparty computation.

Partner 14: University of Bristol (UNIVBRIS) – United Kingdom	
Report on exploitation activities after 3rd 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. Furthermore, results from PRACTICE have fed into other activities related to secure multi-party computation in which UNIVBRIS is involved in, e.g. the HEAT project.
Updated exploitation plan after 3rd 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. Concretely, together with INESC we plan to submit a project proposal to the H2020 programme that builds on research that was carried out within the PRACTICE project.

Partner 15: Distretto Tecnologico Aerospaziale S.C. A R.L. (DTA) – Italy	
Report on exploitation activities after 3rd project year	In the third project year, DTA focused exploitation strategy in applying the methodologies for eliciting data protection requirements in other industrial scenarios. In particular it was defined a new research line, in collaboration with other DTA members, to be pursued in the context of the UAV Test Bed in the Airport of Grottaglie-Taranto. The research is aimed at increasing cyber-security performances of the UAVs and payload data management system that is in its design phase. The UAVs and payload data management system will provide services to customer of the Test Bed. The PRACTICE team of University of Salento is involved in this activity. During this year also several talks were given in national and regional conferences with the aim to raise the interests of industry as well as policy-maker toward the security management in collaborative businesses. Indeed, data protection capabilities is perceived as an obstacle for internationalization of SMEs. Lastly, the team of University of Salento held a number of speeches during face to face meetings with national and international industrial organizations with the objective to add data leakage risk management in the collaboration themes. By leveraging the experience gained in European research and innovation projects, developed participating in the PRACTICE consortium, DTA improved its capacity to operate with an European landscape. With this mind set, DTA joined the European Aerospace Cluster Partnership (EACP) during the last General Meeting (held on 25th and 26th October 2016 in Lisbona). It will be a valuable driver for future European based research and innovation projects.
Updated exploitation plan after 3rd project year including stakeholder	In the next months, the methodology will be applied in the context of design and develop services for UAV Test Bed customers. The University of Salento launched a PhD topic on the security in the aerospace supply chain with the objective to extend the focus of the methodologies in the collaborative product design. The PhD course is planned to start in next December.

Partner 16: Università degli Studi di Milano (UMIL) – Italy	
Report on	**UMIL** has presented the results developed in PRACTICE in several events

Partner 16: Università degli Studi di Milano (UMIL) – Italy	
exploitation activities after 3rd project year	and re-used and extended much of the research work done for the project. 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 3rd project year including stakeholder	The participation to the project and the achieved research results will be used for producing scientific publications, for teaching purposes, for contacting potentially interested partners and companies and propose new collaborations. A number of research activities have been started and the experiences collected during the project duration are being used both for scientific/didactic purposes and more application-oriented partnerships. 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 3rd project year	During the third year, **PAR's** exploitation activities have focused on meetings with stakeholders related to the two MPC applications (survey and benchmarking) as well as potential business partners within Secure Statistics in general. The later, focuses on extending the Partisia team to include competences needed to realize the business potential in Secure Statistics. Both the survey and the benchmarking systems have been used intensively to showcase the potential of Secure Statistics and to include more stakeholders.
Updated exploitation plan after 3rd project year including stakeholder	**PAR** is basically a commercial platform that ultimately transforms R&D in MPC applications into more focused spinouts. Along the way, Partisia sell Software-as-a-Service for auctions and statistics. PRACTICE has been a very important in funding the development of the prototypes needed to attract business partners. The new project (Big Data by Security) funded by the Danish Industry Foundation, complements the work in PRACTICE and improves PARs go-to-market strategy for secure statistics. At present, negotiations with business partners focuses on creating a spinout within the field of Secure Statistics.

Partner 18: Georg-August-Universitaet Goettingen Stiftung oeffentlichen Rechts (UGOE) – Germany	
Report on exploitation activities after 3rd project year	During the third year, **UGOE's** exploitation activities have again been focused on the collection and arrangement of materials (cases, articles, books, especially dealing with the new European General Data Protection Regulation (GDPR)) as a source for articles, reports and conference proceedings concerning legal problems and solutions regarding the project outcomes. The article "Personal Data and Encryption in the European General Data Protection Regulation" has been published in Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 7 (2) 2016, pp. 163-177
Updated exploitation plan after 3rd project year including stakeholder	**UGOE** will continue publishing articles in scientific journals regarding legal aspects of cloud computing and encryption. The results of the research will be disseminated in possible conference proceedings. Together with other partners of the PRACTICE project UGOE will participate in the follow-up H2020 EU project "SODA", starting on 1 January 2017, which deals with privacy preserving computation in a medical big data scenario.

Table 7: Exploitation reports and updated plans

3.4 Joint exploitation strategy (sustainability plan)

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.

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.

The joint exploitation from PRACTICE is best highlighted by the many software components and solutions developed in the project (see Figure 6). Below we list a number of these and describe how these components are important stepping stones for future exploitation of the values created by PRACTICE. Common for these examples is the potential commercial value either directly as software solution or indirectly as components in future software solutions or as stepping stones for research and business collaboration. Common for all of the examples/solutions listed below is that they all involve many stakeholders beyond PRACTICE and form a platform for continuous exploitation.

3.4.1 SEEED - Search over encrypted data

SEEED (**Se**arch ov**e**r **e**ncrypted **d**ata) provides secure storage for sensitive information via encryption. Multiple encryption schemes with different properties are utilized and combined to encrypt the sensitive data in a layered fashion. Hence, enabling the evaluation of SQL queries over the encrypted data by also using property-preserving encryption schemes as well as additive homomorphic encryption.

SAP's SEEED implements all security and infrastructure relevant components identified in this project and outlined in form of the SPEAR & DAGGER framework. It was used to implement PRACTICE's supply chain management use cases in the aerospace industry and vendor managed industry white goods industry in joint collaboration with UWUERZ, DTA/CCII and ARC.

SEEED was presented in multiple internal meetings with SAP's HANA product management to discuss potential product and service integration. Core techniques developed during the evolution of the SEEED prototype, have been adapted for SAP. In addition to this SAP's internal development group is working on a data management system for HANA which supports encryption – and this ongoing work has benefited from the technology developed for SEEED. Furthermore, a technology transfer roadmap was developed for internal stakeholders to assess the complete SEEED solution for their products and the required legal process for software export was initiated.

The developed tools were not only presented to interested internal stakeholders and are prepared to be integrated into products, but will also be further used, improved and exploited in the H2020 projects TREDISEC (Trust-aware, REliable and Distributed Information SEcurity in the Cloud) and ESCUDO-CLOUD (Enforceable Security in the Cloud to Uphold Data Ownership) in which SAP is involved.

3.4.2 Secure Statistics prototypes

The statistical prototypes developed in PRACTICE range from a general survey system to MPC solutions tailored for specific purposes like financial risk assessment and DNA analysis. The prototypes represents prime examples of secure statistics within some of the most regulated industries. The prototypes and associated business cases require a lot of highly sensitive information from a representative sample of individual persons or companies as input to a statistical model. A high level of trust is required to comply with regulation and not least to motivate truthful participation, which is traditionally ensured by a single organisation (and consequently trusted employees in this organisation) that take the role as trustee and use in-house servers to avoid cloud leakages. All prototypes use MPC as a new trust model that simply keep the sensitive information encrypted at all times and with no single point of trust. The security added by MPC provides value directly by allowing the use of cloud computing and by removing the need to buy expensive consultants as trustees. Indirectly, this more agile and cloud based approach to secure statistics allow for more use of sensitive data in a data driven future.

The first prototype built in PRACTICE was the survey system, which has been used for several real-life surveys and been improved throughout the PRACTICE project. The secure survey system provides a new trust model to handle and analyse confidential answers to questionnaires. The most significant use of the survey system has been an employment satisfactory survey conducted by CYBER for the Tartu City Government in Estonia. 80% of the 300 employees participated in the successfully conducted survey and the MPC approach to security was appreciated.
The survey system illustrates the flexibility built-in to the SPEAR & DAGGER architecture. The joint development has resulted in a survey system with the same front-end running on both the Sharemind and the Fresco/SPDZ MPC back-end systems. The two MPC engine also offers different security guarantees. The Fresco/SPDZ runs on two servers and provides active security and Sharemind runs on three servers and provides passive security. This built-in flexibility also has a number of other advantages as explained later in this section.

As oppose to the generic survey system, the two prototypes tailored financial risk assessment and DNA analysis represent another approach to exploitation. In both cases the solutions addresses concrete business cases where secure statistics adds value directly. Also, a high number of stakeholders have been involved in designing and testing the prototypes to ensure that the solutions solve real problems. Altogether, these prototypes form a starting point for actual sale and business development in the field of Secure Statistics.

Common for all of the secure statistics prototypes is that they are built on the SPEAR & DAGGER architecture developed in PRACTICE. The flexibility offered by the SPEAR & DAGGER architecture is particularly evident in the survey prototype that run on two different MPC engines. This decoupling of the front- and backend is highly valuable in many ways for example: 1) it sent a signal to the market that future customers would not be locked-in to vendors, 2) it provides the flexibility needed to continuously include state-of-the-art MPC algorithms, and 3) the frontend development requires less MPC skills, which is important to spread the use of MPC based secure statistics.

The PRACTICE partners that have developed the secure statistics prototypes, all have a dedicated strategy towards commercialisation of MPC in general. Spinout projects and business collaborations from PRACTICE, have already been ensured to continue the basic R&D and business activities needed to get the most out of the secure statistics prototypes developed in PRACTICE. Furthermore, the joint survey prototype functions as a common ground for future collaboration on joint exploitation beyond PRACTICE between the partners CYBER, ALX and PAR. The PRACTICE project has been instrumental and a direct stepping stone for this development.

3.4.3 The PRACTICE Cloud Software Development Ecosystem

Building on the successful SDK, the PRACTICE project is taking a step further in simplifying the adoption of secure computing. Led by CYBER, we have created a service that can take a secure computing app developed with the PRACTICE SDK and easily deploy it on the public cloud. In addition, we are working hard to integrate verification technologies from INESC TEC so that developers can more easily check whether their app inadvertently publishes private data.

The SDK and the service have been designed to address the current complexity barrier of deploying PRACTICE technologies and also shorten the time to market.

Features of the SDK:

1) Develop the secure computing functionality in the privacy-aware, open source SecreC programming language developed by CYBER.
2) Analyse the SecreC code for privacy using the tools from INESC TEC.
3) Get a runtime estimate for secure computing mechanisms in the PRACTICE SPEAR & DAGGER framework. Currently supported are the Sharemind Application Server from CYBER (full integration), ABY from TUDA and FRESCO from ALX (both with partial integration).

Features of the deployment service:

1) Coordinate distributed deployments by setting up the organisation online with invites.
2) Provide a selection from PRACTICE SPEAR & DAGGER secure computing systems to use in the deployment. At the time of the demo, only the Sharemind Application Server from CYBER is fully integrated, but ALX is also working on the deployment mechanisms of FRESCO.
3) Provide assistance to people deploying PRACTICE secure computing systems by integrating with selected cloud providers (e.g., a pre-built virtual machine image or software package that can be installed with a few clicks).
4) Simplified online configuration to improve the user experience or manual offline configuration for extra security and stronger trust guarantees.
5) Potential to build in licensing mechanisms for PRACTICE SPEAR & DAGGER components. For example, the application developer could pay for receiving some licenses and deploy the secure computing component and/or the secure statistics service.

Links to PRACTICE prototype versions of the SDK and the service are available from the PRACTICE website (http://www.practice-project.eu).

3.4.4 SCAPI - Secure Computation API

SCAPI is an open source library for efficient secure multi-library computation that is developed and maintained by BIU. SCAPI includes many state-of-the-art protocols, such as oblivious-transfer extension, and the most recent versions Yao's two-party protocol. These protocols are included in a stable and well-maintained version, and using a consistent API. The library therefore became a useful tool for developing secure computation protocols and applications, and has been used by multiple different projects. While the vast majority of the SCAPI code was developed by BIU, the exploitation of this project is demonstrated by the large number of members in the project. The list of members (based on usage of github) can be found at https://github.com/bennypinkas/scapi/network/members Almost all of these members

are not from BIU or from PRACTICE, but rather users from other organizations.

3.4.5 ABY – A framework for two-party computation

The exploitation strategy of TU Darmstadt as a university partner concentrates mostly on publishing research papers at high-ranked conferences and journals together with the project partners. Participating in and organizing relevant conferences and workshops is also of importance. Besides these, TU Darmstadt provides prototype implementations of protocols designed and optimized through research activities and presented in research papers.

The mixed-protocol secure two-party computation framework developed at TU Darmstadt, ABY, is available as open-source at http://encrypto.de/code/ABY and is being developed continuously. ABY is part of the SPEAR/DAGGER architecture, more specifically implements all components in DAGGER. In the third project year, we have completed a prototype implementation of universal circuits (available open-source at http://encrypto.de/code/UC). This can be used alongside with ABY or any secure computation tool for evaluating any functionality represented by a Boolean circuit in a private manner, i.e., such that one of the parties holds the functionality which is kept private throughout the computation. To demonstrate this, we have implemented private function evaluation in ABY.

The fruitful collaboration between TUDA and BIU on private set intersection resulted in two conference papers and one journal article (in submission). We are continuing this joint research in the future and have applied for a follow-up project together.

As shown by the examples above, TU Darmstadt builds applications on top of the ABY framework and will continue to do so in the future as well, using it in follow-up projects such as CROSSING (Cryptography-Based Security Solutions: Enabling Trust in New and Next Generation Computing Environments), where Ahmad Sadeghi and Thomas Schneider from TUDA are PIs of project E3 on “Compiler for Privacy-Preserving Protocols”, and CRISP (Center for Research in Security and Privacy), that emerged from PRACTICE.

3.5 Concluding remarks

The selected software components and complete SMC applications described above, represent different paths to continues exploitation based on the PRACTICE results. The common SPEAR & DAGGER architecture joins the many activities together in a coherent collective stack. As illustrated in Figure 6 many combinations of the different tools and components can be used to cover the complete SPEAR & DAGGER stack. Each color represents the set of components described above that each makes up a complete SMC solution[3]. As an example, this flexibility is illustrated directly by the complete Secure Survey system, where the same frontend run on two distinct SMC back-ends.

While the SPEAR & DAGGER architecture is an important part to ensure continues joint exploitation, the real challenge is to meet the market in a fruitful way. The large number of end-users involved in the designing, testing as well as actual use of the different PRACTICE applications, have provided valuable feedback for future exploitation. One challenge is the computational overhead that limits the number of applicable use cases. The flexibility of the SPEAR and DAGGER tackle this challenge directly by ease the uptake of new and improved MPC protocols and other components.

However, a number of business opportunities are not hampered by the computational overhead. SMC based auctions have been a commercial activity for years and represent a use case where the computational overhead is neglectable. The many use cases and SMC applications developed in the PRACTICE project represent business opportunities where the

[3] The SCAPI is at an earlier stage than the rest and does not cover to full stack.

computational overhead has little or no influence. Also, in parallel with the PRACTICE project, partners involved in PRACTICE have secured funding from institutional investors for MPC systems used for basic scalable cloud infrastructure such as “key management”.

PRACTICE has paved the road for continuous exploitation and spinout projects that are built directly on the results from PRACTICE. Also, several PRACTICE partners are directly involved in commercial activities that will bring privacy enhancing MPC solutions to the market.

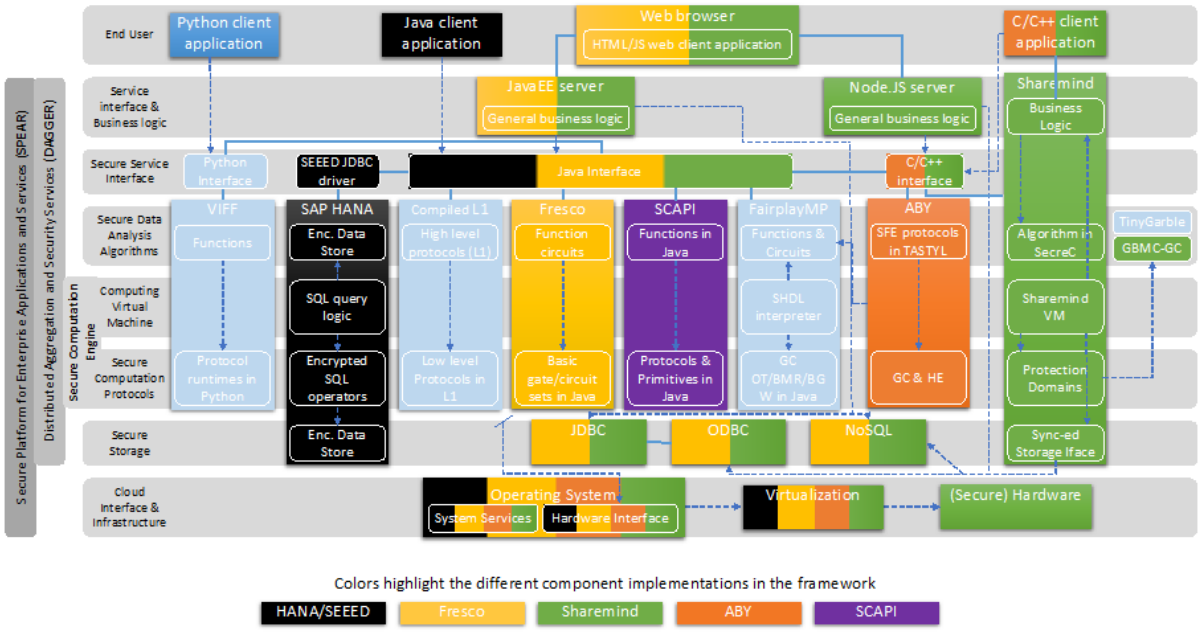

Figure 6: The SPEAR & DAGGER stack and selected combinations of components that constitute complete MPC solutions.

Chapter 4 Internal and external training

4.1 Training activities

During the third year, some effort has still been dedicated to training and education activities dedicates to members and non-members of the PRATICE consortium.

Most training has been carried on in the form of self-training and learning on the job, after that architecture of the project and each individual component has been designed and prototyped. Many individual and non-structured learning activities (researchers learn on-the-job) have been taken and some of the partner talks held during the project meetings have also helped to share knowledge and inspire innovation.

Besides self-training, PRACTICE organized several schools 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 third 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.

4.1.2 Training at schools

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

- Thomas Schneider from TUDA gave a lecture series at the 21st Estonian Winter School in Computer Science (EWSCS), in Palmse, Estonia, February 28 - March 4, 2016 on "Practical secure two-party computation and applications". EWSCS is a series of international winter schools held annually in Estonia. EWSCS are organized by Institute of Cybernetics, a research institute of Tallinn University of Technology. The main objective of EWSCS is to expose Estonian, Baltic, and Nordic graduate students in computer science (but also interested students from elsewhere) to frontline research topics usually not covered within the regular curricula. In the frame of the winter school, about 50 participating students got useful insights about the main topic of PRACTICE: secure multiparty computation and its possible applications.
- TUDA has offered a research seminar on "Privacy-Preserving Technologies" in the winter term 2015/16, where 16 students of TU Darmstadt got the opportunity to become familiar with secure computation technologies. The topics covered both generic secure computation technologies (e.g. privacy-preserving mobile applications, oblivious RAM, private function evaluation) and task-specific protocols (e.g. private set intersection, private information retrieval). Participating students became familiar with their chosen topics, provided a short summary of research papers they have studied and presented their topics to the other students in the form of a seminar. The seminar received excellent feedback and 4 students decided to

write their theses in secure computation technologies already. Therefore, TUDA offers the seminar this winter term 2016/17 again with a larger number of participants.

- AU organized the workshop ³Theory and Practice of Multiparty Computation III² in Aarhus, spring 2016. The workshop had about 125 participants from all over the world and 25 international invited speakers. The workshop was a great scientific success and also had good coverage in the media, including articles in all relevant Danish media for IT professionals. We also had participation from several companies that are developing software for secure computation, thus demonstrating that the area is now truly founded in both theory and practice.
- Manuel Barbosa from INESC Porto gave a lecture at the CUSO Doctoral School in Neuchatel, Switzerland about secure computation relying on trusted hardware supporting isolated execution environments. The event was attended by young researchers from several Swiss universities; in this instance there were about 15 participants.
- UNIVBRIS organised the summer school ``Computer Aided Verification of Cryptographic Protocols" in September 2016. The school addressed different methods for verifiability of protocols, including those for verifiable computation have been presented. The school was attended by about 40 students and featured speakers from France, UK, and Spain.

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.
The effort of the partners involved in these activities has concretized in the realization of a large quantity of actions as reported in the previous sections. Table 8: Summary of main activities in the three years below, summarizes the main activities performed in the three years of the project. The numbers that confirm the involvement of the members are supported 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.
In these three years, standardization 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 result. 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
We highlight here the exploitation activities that are reported as the successful experiences by some of the partners, as well as the joint exploitation actions that 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.

Dissemination, standardization, exploitation and training activities	Year 1 (M01-M12)	Year 2 (M13-M24)	Year 3 (M25-M36)	Total
Number of peer-reviewed scientific publications	18	26	19	63
Number of public deliverables	7	10	9	26
Number of presentations, conferences, workshops, summer schools and other events	23	35	31	89
Website visitors	5.679	47.073	52.426	105.178
Number of patents	-	1	-	1
Number of exploitation stories	-	3	4	4
Number of standardisation activities	2	3	3	8
Number of training activities	6	9	9	24

Table 8: Summary of main activities in the three years