D32.1

Updated plan and initial report on dissemination, standardisation, exploitation and training

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

Deliverable type:	Report
Deliverable reference number:	ICT-609611 / D32.1 / 1.0
Activity and Work package contributing to the deliverable:	Activity 3 / WP32
Due date:	October 2014 – M12
Actual submission date:	22nd February, 2015

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

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

Editor

Stelvio Cimato (UMIL),

Contributors (ordered according to beneficiary numbers)

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

Disclaimer

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

Executive Summary

This deliverable reports on the progress of the project partners in terms of dissemination of the project, standardisation and exploitation of project results, and project internal/external training during the first year of the PRACTICE project. It further describes the planned future activities in those areas during the remainder of the project duration. As IPR (Intellectual Property Rights) issues are directly related to exploitation activities, they are covered within this deliverable.

In particular, the deliverables accentuates the impact of the project in the international cloud computing research community through scientific publications on high-quality, international conferences and the organisation of events that attracted well renowned researchers in this area. Moreover, it provides an overview of the PRACTICE potential to international standardization initiatives.

Furthermore, this deliverable reports on already delivered and planned training and educational measures. The training occurred on the one hand project-internally in order to achieve a common technological knowledge base among the project partners. And on the other hand project externally, e.g., within the education at the academic partners.

To further raise the public level of awareness of the project within the scientific and industrial communities, a diversity of dissemination activities have been impelled, including a project website with blog and twitter and presentations at workshops and conferences.

The following falls under the achievements and work towards the project goals of the first project year for dissemination and standardisation:

- 18 peer-reviewed scientific publications
- 15 organized events (workshops, summer schools) with an international audience and very good feedback as well as organization (or involvement in the organisation) of high-profile international events.
- Partners participated in 8 conferences including partly presentations
- A thorough survey of standardisation opportunities and first contact with the standardisation bodies.

We performed the following changes in V1.1 of D32.1 - Updated plan and initial report on dissemination, standardisation, exploitation and training:

- Section 1.1.1 - Audience and Evaluation Criteria is novel.
- Section 1.2.2 and Table 3 have been modified to include the target audience.
- Section 3.2 includes individual partner tables where a detailed report of exploitation activities is listed.

Disclaimer

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

Contents

List of Figures

List of Tables

Chapter 1 Dissemination

Dissemination activities are provided to ensure the visibility and awareness of the project and to support the widest adoption of its results in industry and research. The strategy for the dissemination of PRACTICE aims at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties. This document presents the initial dissemination strategy and reports on all the dissemination activities already executed during the first year. The strategy will be updated and reported during the course of the project, and monitoring activities will be performed in order to check the success of the dissemination plan and to adapt if necessary the actions to the changing needs.

1.1 Dissemination Strategy

The PRACTICE dissemination strategy adopted for the entire project duration is based 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).
- Backing by robust infrastructure (Section 1.2.3).
- Presentation of the project to the general public (press, web, etc.), Section 1.2.4:
    - 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
    - A public project website was installed and maintained. In addition, some partners have dedicated one page on their website to explain the project and their involvement
        - http://www.technikon.com/projects/practice
        - https://www.trust.informatik.tu-darmstadt.de/research/projects/current-projects/practice-privacy-preserving-computation-in-the-cloud/
        - http://www.bwl.uni-wuerzburg.de/lehrstuehle/bwl11/research/research_topics/supply_chain_collaboration/
        - http://www.alexandra.dk/dk/cases/sider/practice.aspx
        - http://dtascarl.it/progetti/45-practice.html
    - At the end of the project the results can be presented to journalists (dedicated press tour or during the above road show)
    - Mention the project on the website of the FP7 HiPEAC network of excellence

1.1.1 Audience and Evaluation Criteria

The main objectives of the dissemination activities are the creation of external awareness of the project, and the communication of the project's research results and benefits to all the potentially interested stakeholders. The communication on the project and its results have to be directed to targeted audience in order to select the most appropriate channels and to reach the largest number of interested people.

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

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

Scientific community includes academics, PhD students, and IT researchers. The strategy to reach this group will be based on scientific publications and presence in academic events or conferences. Commercial dissemination aims to raise awareness and inspire interest and market demand, involving Business Decision Makers and Specialists as end users of the case studies – supply chain management and financial analysis – being developed in the project; IT Decision Makers implementing cloud computing in enterprise IT infrastructures, who could benefit of project results to face with security and privacy challenges; and Developers, who could integrate the provided solutions into their offering.The consortium will participate in a number of events and organize a number of outreach activities in order to interact with the eventual beneficiaries of the PRACTICE technology. Finally, the strategy to reach wide audience is to use the website and other communication means such as blogs, social networks (Twitter, LinkedIN, etc.) newsletters, and produce dissemination materials easily accessible from different channels.

To evaluate the effect that strategies have on getting the message to the audience a number of Key Performance Indicators (KPI) have to be selected, so that progress towards fixed goals for dissemination activities can be effectively measured. The following table collects the selected KPI:

Dissemination activity/channel	KPI
Website	• Number of visits • Number of unique visitors
Scientific Conferences and Journals	• Number of publications per year • Number of attendees • Impact factor • Feedback received • Number of citations
Newsletters/Fact Sheets/Posters	• Number of contacts • Number of downloads
Social Networks/Blogs	• Number of contacts • Number of posts/messages
Presentation/Workshops	• Number of attendees • Number of events

Table 1: Key performance indicators for the dissemination activities

A periodic monitoring of these KPIs will be started to ensure that dissemination activities are successfully executed, and errors in the dissemination plan can be easily detected and appropriate countermeasures undertaken.

1.2 Dissemination Activities Started in M01-M12

The project and its results have been disseminated by invited talks at conferences, by publications at scientific and industry oriented conferences (such as ACNS, USENIX Security, CRYPTO, Computer and Communications Security) 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 first PRACTICE project year. All scientific publications are listed in an action overview list and are updated by the partners on a regularly base. Currently 18 peer-reviewed scientific publications were prepared during the first project year.

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Publicly Auditable Secure Multi-Party Computation	Carsten Baum, Ivan Damgård, Claudio Orlandi	SCN	Springer	Amalfi	2014	http://eprint.iacr.org/2014/075	No
An Empirical Study and Some Improvements of the MiniMac Protocol for Secure Computation.	Ivan Damgård, Rasmus Lauritsen, Tomas Toft	SCN	Springer	Amalfi	2014	http://eprint.iacr.org/2014/289	No
Faster Maliciously Secure Two-Party Computation Using the GPU	Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen	SCN	Springer	Amalfi	2014	http://eprint.iacr.org/2014/270	No

[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	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
A Framework for Outsourcing of Secure Computation	Thomas P Jakobsen, Jesper Buus Nielsen, Claudio Orlandi	ACM Cloud Computing Security Workshop (CCSW)	ACM	Arizona (USA)	2014	-	No
Automatic protocol selection in secure two-party computations	Florian Kerschbaum, Thomas Schneider, Axel Schröpfer	Applied Cryptography and Network Security (ACNS)	Springer	Berlin	2014	http://eprint.iacr.org/2014/200	Yes
GSHADE: Faster privacy-preserving distance computation and biometric identification	Julien Bringer, Hervé Chabanne, Mélanie Favre, Alain Patey, Thomas Schneider, Michael Zohner	ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC)	ACM	New York	2014	http://dl.acm.org/citation.cfm?doid=2600918.2600922	No
Notes on non-interactive secure comparison in "Image feature extraction in the encrypted domain with privacy-preserving SIFT"	Matthias Schneider, Thomas Schneider	ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC)	ACM	New York	2014	http://dl.acm.org/citation.cfm?doid=2600918.2600927	No
Faster private set intersection based on OT extension	Benny Pinkas, Thomas Schneider, Michael Zohner	USENIX Security Symposium (USENIX Security)	USENIX	San Diego (CA)	2014	http://eprint.iacr.org/2014/447	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Ad-hoc secure two-party computation on mobile devices using hardware tokens	Daniel Demmler, Thomas Schneider, Michael Zohner	USENIX Security Symposium (USENIX Security)	USENIX	San Diego (CA)	2014	https://eprint.iacr.org/2014/467	Yes
Cut-and Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings	Yehuda Lindell, Ben Riva	CRYPTO 2014	CRYPTO 2014	Santa Barbara (CA)	2014	http://dx.doi.org/10.1007/978-3-662-44381-1_27	Yes
Compact Ring-LWE Cryptoprocessor	Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Donglong Chen, Ingrid Verbauwhede	Workshop on Cryptographic Hardware and Embedded Systems (CHES)	CHES	Busan (Korea)	2014	https://eprint.iacr.org/2013/866.pdf	Yes
Searchable Encryption with Secure Efficient Updates	Florian Hahn, Florian Kerschbaum	ACM Conference on Computer and Communications Security (CCS)	ACM	Arizona (USA)	2014	-	No
Optimal Average-Complexity Ideal-Security Order-Preserving Encryption	Florian Kerschbaum, Axel Schröpfer	ACM Conference on Computer and Communications Security (CCS)	ACM	Arizona (USA)	2014	-	Yes

Title	Main authors	Title of the periodical or the series	Publisher	Place of publication	Year of publication	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
Tutorial: Client-Controlled Cloud Encryption	Florian Kerschbaum	ACM Conference on Computer and Communications Security (CCS)	ACM	Arizona (USA)	2014	-	Yes
RAID-PIR: Practical multi-server PIR	Daniel Demmler, Amir Herzberg, Thomas Schneider	ACM Cloud Computing Security Workshop (CCSW)	ACM	Arizona (USA)	2014	http://dx.doi.org/10.1145/2664168.2664181	No
Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices	Markus Miettinen, N. Asokan, Thien Duc Nguyen and Ahmad-Reza Sadeghi	ACM Conference on Computer and Communications Security (CCS)	ACM	Arizona (USA)	2014	-	No
ASM: A Programmable Interface for Extending Android Security	Stephan Heuser, Adwait Nadkarni, William Enck and Ahmad-Reza Sadeghi	USENIX Security Symposium (USENIX Security)	USENIX	San Diego (CA)	2014	-	Yes
Swap and Play: Live Updating Hypervisors and Its Application to Xen	Franz Ferdinand Brasser; Mihai Bucicoiu; Ahmad-Reza Sadeghi	ACM Cloud Computing Security Workshop (CCSW)	ACM	Arizona (USA)	2014	-	No
Homomorphic Signatures with Efficient Verification for Polynomial Functions	Dario Catalano, Dario Fiore, and Bogdan Warinschi	Crypto 2014	Springer	Santa Barbara (CA)	2014	https://eprint.iacr.org/2014/469	Yes

Table 2: List of publications

1.2.2 Presentations, Conferences and Workshops

All Presentations, Conferences and Workshops are listed in an action overview list and are updated by the partners on a regularly base. Currently the PRACTICE partners participated in 27 presentations, conferences and workshops during the first project year. Most of the activities have focused on presentation to scientific conference and workshops. Dissemination targeted to commercial audience and industry expert will be increased in the second year when practical results and prototypes could be presented. 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/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
Workshop/Scientific	Intel, TEC	Participation in the Plenary of the EU Platform on Network and Information Security	11	12	2013	Brussels	80	Promotion of PRACTICE goals within EU Research community.	International
Workshop/Scientific	Intel, TEC	Participation in the WG3 (Research and Innovation) of the EU Platform on Network and Information Security	12	12	2013	Brussels	40	Promotion of cloud privacy as an important challenge for future research	International
Workshop/Scientific	TEC	Cluster Workshop on Cyber Security in FP7 Security & Trust Research Projects	12	12	2013	Brussels / Belgium	N/A	The main objectives of the meeting were the following: - Positioning security projects and clusters compared to EU cyber security strategies - Introduce new security projects (e.g. call 10 EU funded, national projects) to extend the reach of clusters.	International
Conference/Scientific	SAP	International Conference on Information Systems Security (ICISS)	19	12	2013	Kokata / India	N/A	ICISS (International Conference on Information Systems Security), provides a forum for discussing and disseminating recent advances in information and systems security. ICISS 2014 encourages submissions from the academia, industry and government addressing both theoretical and practical problems in information systems security and	International

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
								related areas.	
Presentation/ Scientific-Commercial	CYBER	Secure Shared Computation in the Public Cloud	14	1	2014	New York	300	Annual Real World Crypto Workshop brings together cryptography researchers and developers implementing real-world systems	International
Workshop/Scientific-Commercial	CYBER,BIU, PAR, AU	Real World Crypto Workshop	13-15	1	2014	New York	300	Annual Workshop bridging academia and industry	International
Workshop/Scientific	AU	Workshop on Applied Multi-Party Computation	20-21	1	2014	Redmond, USA	N/A	The goal of this workshop is to bring together researchers in security and cryptography to discuss recent advances, challenges and research directions related to applied secure computation. The workshop consists of invited keynote presentations, contributed presentations and round-table discussions on all aspects of applied secure computation.	International
Workshop/Scientific	BIU, AU	4th Bar-Ilan Winter School on Cryptography - Symmetric Encryption in Theory and Practice	27-30	2	2014	Ramat Gan / Israel	N/A	Provide a broad basis in the theoretical foundations of symmetric encryption, practical constructions and cryptanalysis	International
Presentation/ Scientific	BIU	On the Performance of Private Set Intersection	3	3	2014	Hebrew University, Jerusalem, Israel	N/A	Presentation of: On the Performance of Private Set Intersection	International
Workshop/Scientific	AU	19th Estonian Winter School in Computer Science (EWSCS)	2-7	3	2014	Palmse, Estonia	N/A	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.	International

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
Workshop/Scientific	TUDA	DIMACS Workshop on Secure Cloud Computing	27-28	3	2014	New Jersey / USA	30	The purpose of this workshop is to advance the current state of the art in secure cloud computing with experts from academia and industry.	International
Conference/Scientific-Commercial	CYBER	Regular meeting of ISO/IEC JTC1 SC27	7	4	2014	Hong Kong SAR / China	~50	Cybernetica was presenting the PRACTICE project to ISO/IEC JTC1 SC 27 to involve the project closer into standardization activities.	International
Conference/Commercial	CYBER	New Frontiers for European Entrepreneurs	29	4	2014	Brussels / Belgium	~300	Cybernetica was included in EU-s Innovation Radar pilot project and was invited to the event. The event - "New Frontiers for European Entrepreneurs" – is bringing together over 100 high growth ICT startups from across Europe together as well leading ICT incubators, accelerators, investors and clusters for networking and collaboration. The "innovation radar" pilot is working closely with the organisers of the event to have meaningful, relevant and targeted activities during the event for each of the innovators, such as your organisation, that we have identified in our pilot.	International
Workshop/Scientific	AU, BIU, TUDA	Theory and Practice of Secure Mulitparty Computation	5-9	5	2014	Aarhus / Denmark	N/A	Secure Multiparty Computation is a powerful cryptographic notion that - in theory - can solve virtually any cryptographic protocol problem. This workshop brings together people in both theory and practice of the field, and we are convinced that this will prove very productive.	International
Workshop/Scientific	CYBER	IARPA SPAR-MPC workshop	28-29	5	2014	Boston / USA	~50	The workshop brought together a state of the art of secure multi-party computation researchers. Cybernetica was discussing a prototype developed within the PRACTICE program.	International
Workshop/Scientific	TUDA, INTEL	Intelligent Things, Vehicles and Factories:	10-11	6	2014	Darmstadt/Germany	150	Presentation of results and future plans in form of Talks, Posters and Demos	Germany, US, Italy, Finland, Romania,

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
		Intel Workshop on Cyberphysical and Mobile Security							Spain, etc.
Conference/Scientific	SAP	12th International Conference on Applied Cryptography and Network Security	10-13	6	2014	Lausanne / Switzerland	N/A	The conference seeks submissions from academia, industry, and government presenting novel research on all aspects of applied cryptography as well as network security and privacy.	International
Workshop/Scientific	TUDA	2nd ACM Workshop on Information Hiding and Multimedia Security (ICH&MMSEC'14)	11-13	6	2014	Salzburg / Austria	> 50	The 2nd Information Hiding and Multimedia Security Workshop focusses on both, information hiding topics such as watermarking, steganography and steganalysis, anonymity, privacy, hard-to-intercept communications, and covert/subliminal channels as well as multimedia security topics such as data hiding, robust/perceptual hashing, biometrics, video surveillance, and multimedia forensics.	International
Conference/Scientific	SAP	ACM Symposium on Access Control Models and Technologies (SACMAT)	25-27	6	2014	London, Ontario / Canada	N/A	The aims of the symposium are to share novel access control solutions that fulfil the needs of heterogeneous applications and environments, and to identify new directions for future research and development.	International
Workshop/Scientific	CYBER	Workshop on Genome Privacy	15	7	2014	Amsterdam / Netherlands		As a result of the rapid evolution in genomic research, substantial progress is expected in terms of improved diagnoses and better preventive medicine. The low cost of DNA sequencing will break the physician/patient connection, because private citizens (from anywhere in the world) can have their genome sequenced without involving their family doctor. An undesirable consequence of this technical progress is that genomics is becoming the next major challenge for privacy, because (i) genetic	International

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
								diseases can be unveiled, (ii) the propensity to develop specific diseases (such as Alzheimer's) can be revealed, (iii) a volunteer, accepting to have his genomic code made public (as has already happened), can leak substantial information about his ethnic heritage and the genomic data of his relatives, and (iv) complex privacy issues can arise if DNA analysis is used for criminal investigations and medical purposes. Such issues could lead to genetic discrimination.	
Workshop/Scientific	UNIVBRIS	Cryptography Summer School	21-24	7	2014	Bucharest / Romania	N/A	The school aims to introduce the participants to the principles of modern cryptography as applied to the most basic primitives. The target audience are top undergraduate and graduate students, early career researchers, as well as security professionals with an interest in cryptography. While no specific prior knowledge on cryptography is required, the participants are expected to be familiar with basic algebra and probability theory.	International
Presentation/ Scientific	BIU	Faster Private Set Intersection Based on OT Extension	14	8	2014	Yorktown, New York, NY	N/A	Presentation of: Faster Private Set Intersection Based on OT Extension	International
Conference/Scientific	BIU, AU	CRYPTO 2014	17-21	8	2014	Santa Barbara (CA) / USA	N/A	CRYPTO 2014 is the 34rd International Cryptology Conference. It will be held at the University of California, Santa Barbara (UCSB) from August 17 to 21, 2014. The academic program covers all aspects of cryptology. The conference is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Computer Science Department of UCSB.	International
Conference/Scientific	BIU, TUDA	23rd USENIX Security Symposium	20-22	8	2014	San Diego, CA / USA	520	The USENIX Security Symposium brings together researchers, practitioners, systems programmers and engineers, and others	International

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
								interested in the latest advances in the security of computer systems and networks. The Symposium will be held August 20–22, 2014, in San Diego, CA, and includes a technical program with refereed papers, invited talks, posters, panel discussions, and Birds-of-a-Feather sessions.	
Conference/Scientific	AU	9th Conference on Security and Cryptography for Networks	3-5	9	2014	Amalfi, Italy	N/A	The Ninth Conference on Security and Cryptography for Networks (SCN 2014) aims at bringing together researchers in the field of cryptography and information security, practitioners, developers, and users to foster cooperation, exchange techniques, tools, experiences and ideas. The conference seeks submissions from academia, government, and industry presenting novel research on all practical and theoretical aspects of cryptography and information security. The primary focus is on original, high quality, unpublished research of theoretical and practical impact, including concepts, techniques, applications and practical experiences.	
Workshop/Scientific	CYBER, TUDA, TUE	Usable and Efficient Secure Multiparty Computation	11	9	2014	Wroclaw / Poland	N/A	Secure Multiparty Computation (SMC) is a universally applicable privacy-enhancing technology, that can be used whenever untrusted platforms compute on sensitive data. The goal of the workshop is to bring together researchers of SMC and builders of secure systems, to discuss the secure computation techniques necessary for practical applications.	International
Conference/Scientific	CYBER	Regular meeting of ISO/IEC JTC1 SC27	20-24	10	2014	Mexico City, Mexico	~50	Cybernetica represented PRACTICE comments to ISO/IEC 19582-1, 19592-2 and 29151. The majority of the comments were accepted and PRACTICE work will be included in the next drafts of these standards.	International

Type of activities/Dissemintation target	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
Presentation/ Commercial	SAP	SAP DKOM				Palo Alto, USA		SAP presented at a highly coveted spot at SAP DKOM in Palo Alto to the entire product development organization.	

Table 3: Presentations, Conferences and Workshops

1.2.3 PRACTICE Project Website

1.2.3.1 Public PRACTICE Website http://www.practice-project.eu

For the purpose of visibility, the project website was launched in month two of the project. It provides an overview of the project and up-to-date information on its activities and results, as well as contact details, information on partners and events. The website is based on the Content Management System (CMS) "Joomla!", a webserver which provides the public website and additionally restricted areas for members only. The website can be viewed with a standard web browser and will be kept alive throughout the project period and at least 3 years afterwards. Our website has been designed such that it can be handled intuitively and gives an introduction to the technical and organisational aspects of the project.

The project website has been updated continuously by the Project Coordinator, whereas all partners participate in the process by notifying the Coordinator of important news and developments.

The following illustration (Figure 1) shows the Welcome page of the PRACTICE website. Project details of PRACTICE as well as the content of the respective section are given.

Figure 1: Welcome page of the PRACTICE website

The structure of the official part of the website includes the following Links:

About

- General introduction about the project including a submenu for further specific information belonging to PRACTICE (mission, motivation, planned results, technical approach, fundamental technologies, progress and expected impact)

News

- Divided in three sub items:
    - Press & News – including press releases (e.g. PRACTICE Leaflet or Newsletter)
    - Conferences & Workshops – list of all past and upcoming conferences and workshops
    - Meetings – list of all past and upcoming meetings

Publications & Deliverables

- Publications by PRACTICE partners (Public and approved Deliverables, other Publications, e.g. PRACTICE application scenarios)

Blog:

- Legal notices (Disclaimer, Legal notices, Privacy and Feedback)
- Blog entries to News, Publications and Events

Links:

- PRACTICE related / relevant projects

Partners

- Consortium of the PRACTICE project

Login

- Login area for project internal use.

The project website serves as the most versatile information and communication tool, as on one hand it provides information for a worldwide audience and on the other hand it enables a working platform for the project team. Therefore, it provides a user-friendly and informative environment.

As mentioned above, the website offers the users general information about the PRACTICE project, its activities, achievements as well as background information, contact details and events. The menu item “News” includes the three sub items “Press & News”, “Conferences & Workshops” and “Meetings”.

Behind this sub items, there is for example a list of all past and upcoming conferences, workshops and meetings as well as press releases as illustrated in the following figures (Figure 2, Figure 3 and Figure 4). The user can access the adequate site of the preferred news. Publications and application scenarios can be found by clicking the “Publications & Deliverables” –menu item. Furthermore publications can be downloaded and useful links are given, which is illustrated in Figure 5.

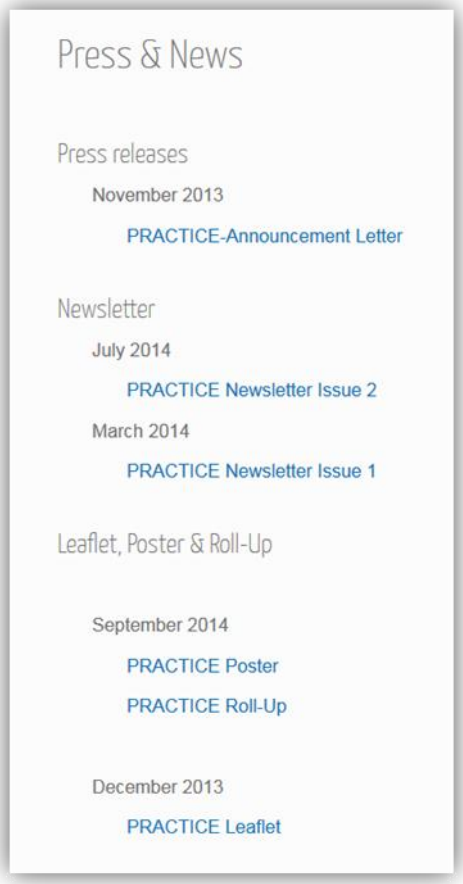
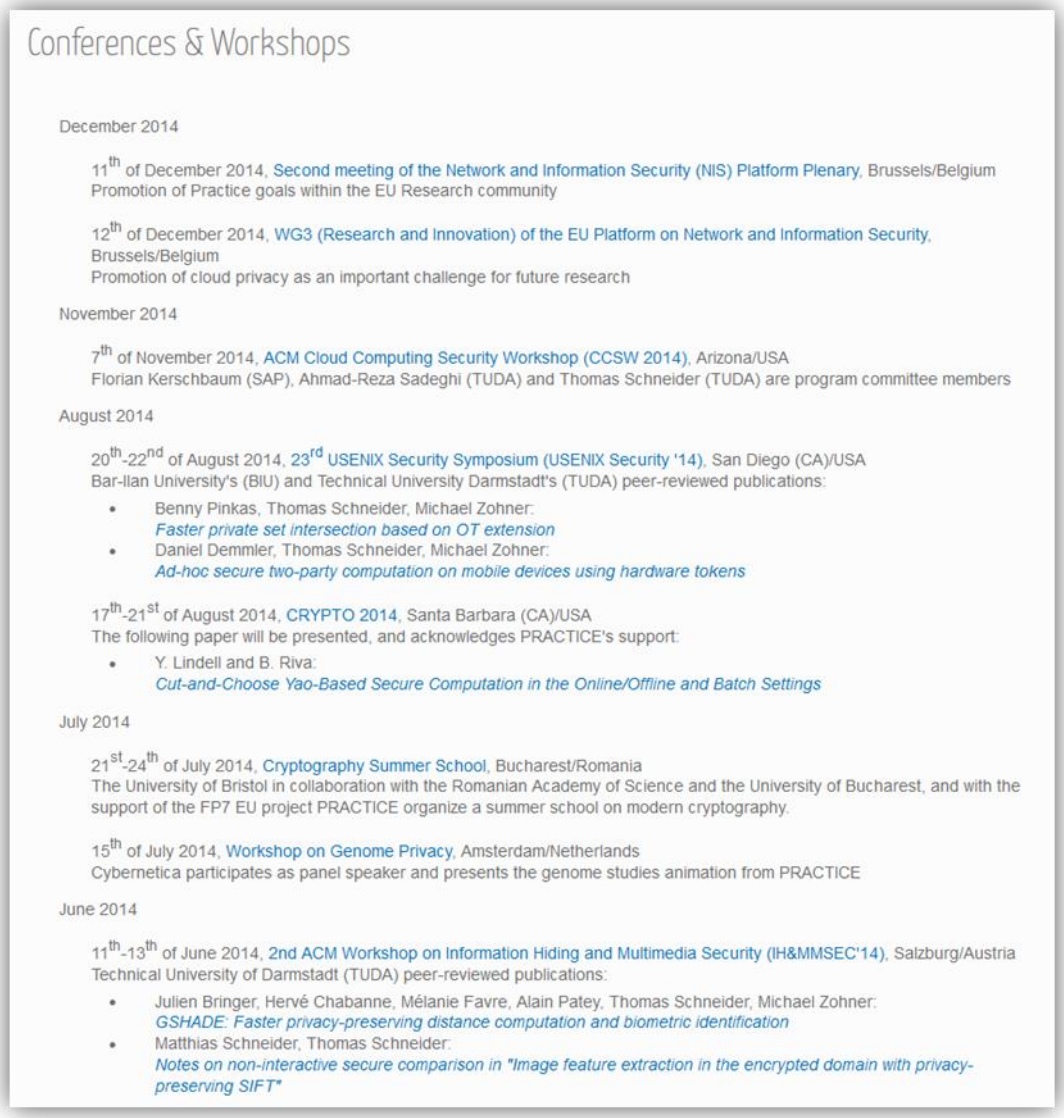


Figure 2: “Press & News”-page of the PRACTICE website



Conferences & Workshops

December 2014

11th of December 2014, Second meeting of the Network and Information Security (NIS) Platform Plenary, Brussels/Belgium
Promotion of Practice goals within the EU Research community

12th of December 2014, WG3 (Research and Innovation) of the EU Platform on Network and Information Security, Brussels/Belgium
Promotion of cloud privacy as an important challenge for future research

November 2014

7th of November 2014, ACM Cloud Computing Security Workshop (CCSW 2014), Arizona/USA
Florian Kerschbaum (SAP), Ahmad-Reza Sadeghi (TUDA) and Thomas Schneider (TUDA) are program committee members

August 2014

20th-22nd of August 2014, 23rd USENIX Security Symposium (USENIX Security '14), San Diego (CA)/USA
Bar-Ilan University's (BIU) and Technical University Darmstadt's (TUDA) peer-reviewed publications:

- Benny Pinkas, Thomas Schneider, Michael Zohner:
  Faster private set intersection based on OT extension
- Daniel Demmler, Thomas Schneider, Michael Zohner:
  Ad-hoc secure two-party computation on mobile devices using hardware tokens

17th-21st of August 2014, CRYPTO 2014, Santa Barbara (CA)/USA
The following paper will be presented, and acknowledges PRACTICE's support:

- Y. Lindell and B. Riva:
  Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings

July 2014

21st-24th of July 2014, Cryptography Summer School, Bucharest/Romania
The University of Bristol in collaboration with the Romanian Academy of Science and the University of Bucharest, and with the support of the FP7 EU project PRACTICE organize a summer school on modern cryptography.

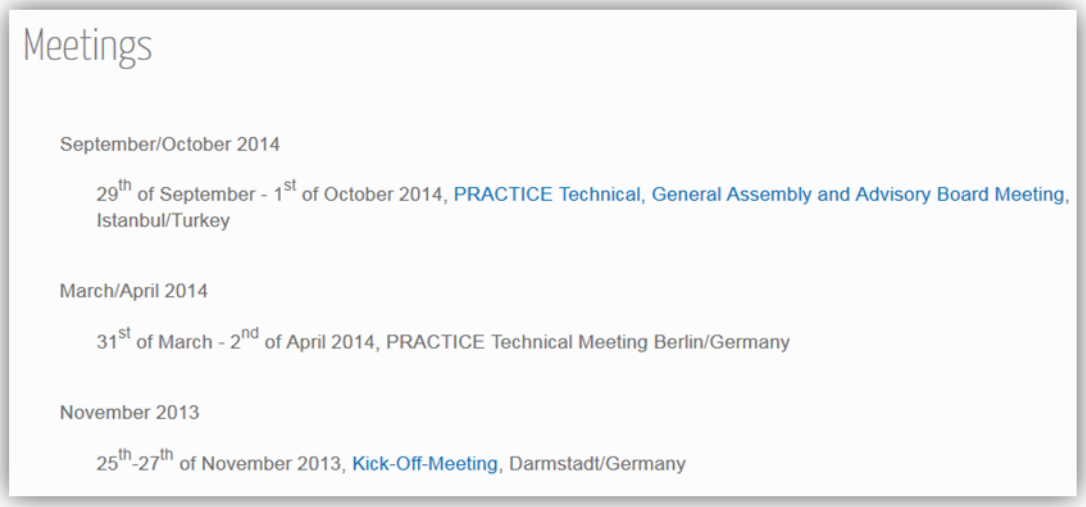
15th of July 2014, Workshop on Genome Privacy, Amsterdam/Netherlands
Cybernetica participates as panel speaker and presents the genome studies animation from PRACTICE

June 2014

11th-13th of June 2014, 2nd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14), Salzburg/Austria
Technical University of Darmstadt (TUDA) peer-reviewed publications:

- Julien Bringer, Hervé Chabanne, Mélanie Favre, Alain Patey, Thomas Schneider, Michael Zohner:
  GSHADE: Faster privacy-preserving distance computation and biometric identification
- Matthias Schneider, Thomas Schneider:
  Notes on non-interactive secure comparison in "Image feature extraction in the encrypted domain with privacy-preserving SIFT"

Figure 3: “Conferences & Workshops”-page of the PRACTICE website



Meetings

September/October 2014

29th of September - 1st of October 2014, PRACTICE Technical, General Assembly and Advisory Board Meeting, Istanbul/Turkey

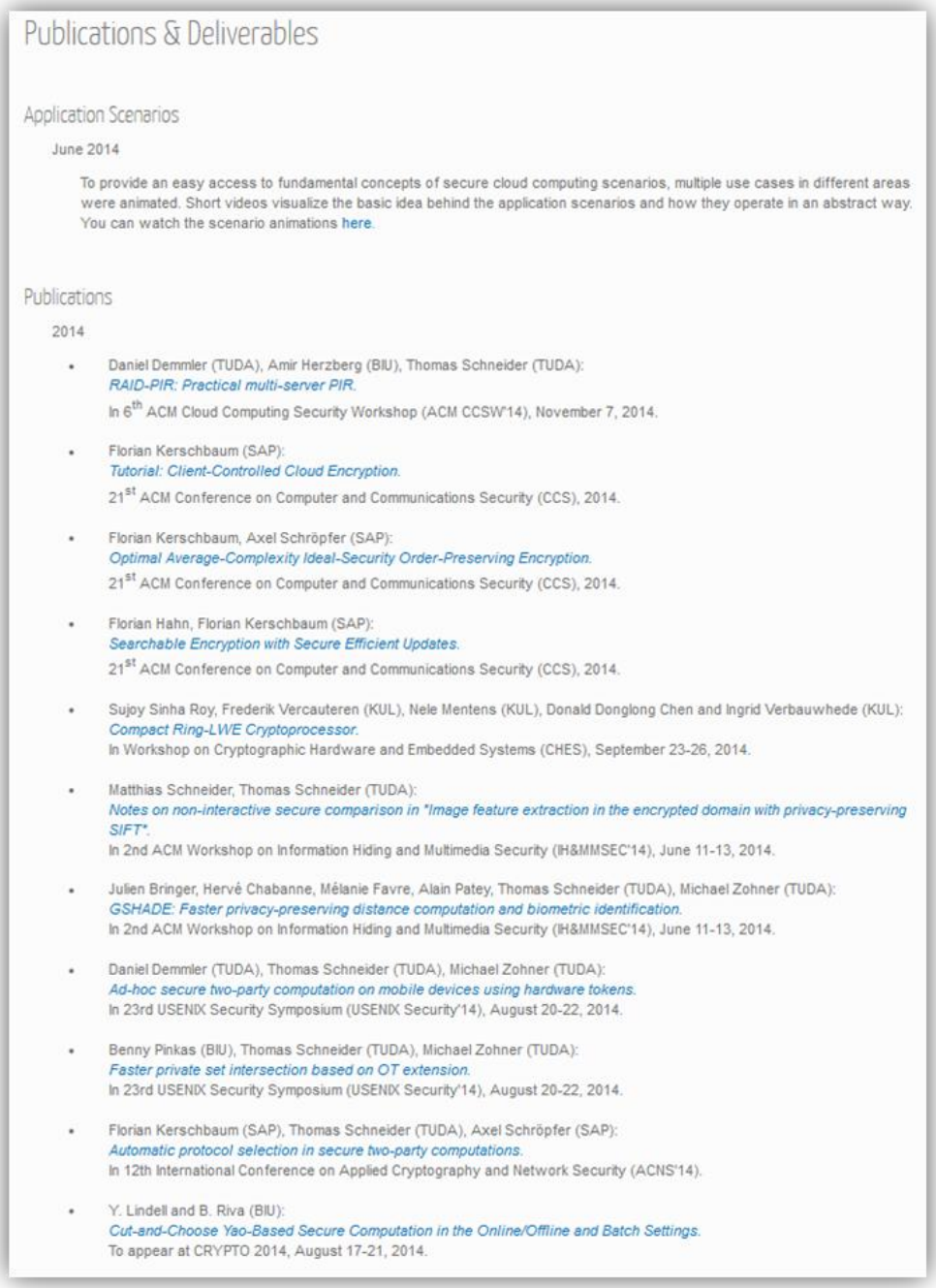
March/April 2014

31st of March - 2nd of April 2014, PRACTICE Technical Meeting Berlin/Germany

November 2013

25th-27th of November 2013, Kick-Off-Meeting, Darmstadt/Germany

Figure 4: “Meetings”-page of the PRACTICE website



Publications & Deliverables

Application Scenarios

June 2014

To provide an easy access to fundamental concepts of secure cloud computing scenarios, multiple use cases in different areas were animated. Short videos visualize the basic idea behind the application scenarios and how they operate in an abstract way. You can watch the scenario animations here.

Publications

2014

- Daniel Demmler (TUDA), Amir Herzberg (BIU), Thomas Schneider (TUDA):
  RAID-PIR: Practical multi-server PIR.
  In 6th ACM Cloud Computing Security Workshop (ACM CCSW'14), November 7, 2014.
- Florian Kerschbaum (SAP):
  Tutorial: Client-Controlled Cloud Encryption.
  21st ACM Conference on Computer and Communications Security (CCS), 2014.
- Florian Kerschbaum, Axel Schröpfer (SAP):
  Optimal Average-Complexity Ideal-Security Order-Preserving Encryption.
  21st ACM Conference on Computer and Communications Security (CCS), 2014.
- Florian Hahn, Florian Kerschbaum (SAP):
  Searchable Encryption with Secure Efficient Updates.
  21st ACM Conference on Computer and Communications Security (CCS), 2014.
- Sujoy Sinha Roy, Frederik Vercauteren (KUL), Nele Mentens (KUL), Donald Donglong Chen and Ingrid Verbauwhede (KUL):
  Compact Ring-LWE Cryptoprocessor.
  In Workshop on Cryptographic Hardware and Embedded Systems (CHES), September 23-26, 2014.
- Matthias Schneider, Thomas Schneider (TUDA):
  Notes on non-interactive secure comparison in "Image feature extraction in the encrypted domain with privacy-preserving SIFT".
  In 2nd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14), June 11-13, 2014.
- Julien Bringer, Hervé Chabanne, Mélanie Favre, Alain Patey, Thomas Schneider (TUDA), Michael Zohner (TUDA):
  GSHADE: Faster privacy-preserving distance computation and biometric identification.
  In 2nd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14), June 11-13, 2014.
- Daniel Demmler (TUDA), Thomas Schneider (TUDA), Michael Zohner (TUDA):
  Ad-hoc secure two-party computation on mobile devices using hardware tokens.
  In 23rd USENIX Security Symposium (USENIX Security'14), August 20-22, 2014.
- Benny Pinkas (BIU), Thomas Schneider (TUDA), Michael Zohner (TUDA):
  Faster private set intersection based on OT extension.
  In 23rd USENIX Security Symposium (USENIX Security'14), August 20-22, 2014.
- Florian Kerschbaum (SAP), Thomas Schneider (TUDA), Axel Schröpfer (SAP):
  Automatic protocol selection in secure two-party computations.
  In 12th International Conference on Applied Cryptography and Network Security (ACNS'14).
- Y. Lindell and B. Riva (BIU):
  Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings.
  To appear at CRYPTO 2014, August 17-21, 2014.

Figure 5: Publications page of the PRACTICE website

A statistical analysis of access (both unique visitors and overall visits) to the PRACTICE project website has been visualized and is shown in the graphics below. In order to obtain these figures, we used two different statistical tools.

The statistical graphics give attention to the M12 in the first project period (1st to 29th of October 2014).

The illustration below provides an overview of the number of unique visitors and the total number of page 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.

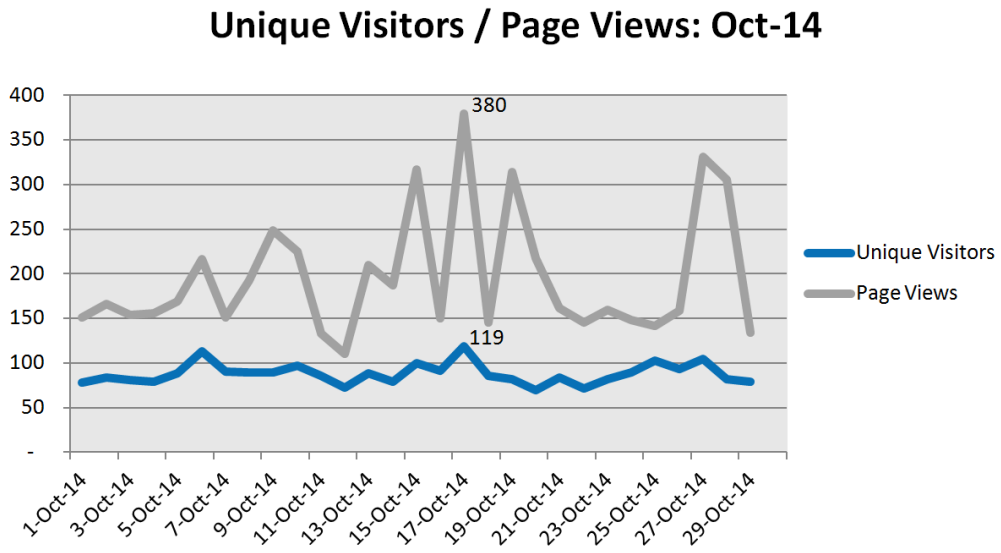


Figure 6: PRACTICE website statistic of unique visitors and non-unique visits

During the whole M12 in the first project period the PRACTICE website has been visited 5,679 times in total by 2,548 unique visitors.

The following website statistic illustrates the geographical distribution of the visitor's location. Three quarters of the visitors were from European region. The remaining percentage is spread over America (North and South America), Asia, Africa and others. This shows that the major interest in this European research project lies of course within Europe. However, it must also be highlighted that the project raises considerable interest among other continents, especially America.

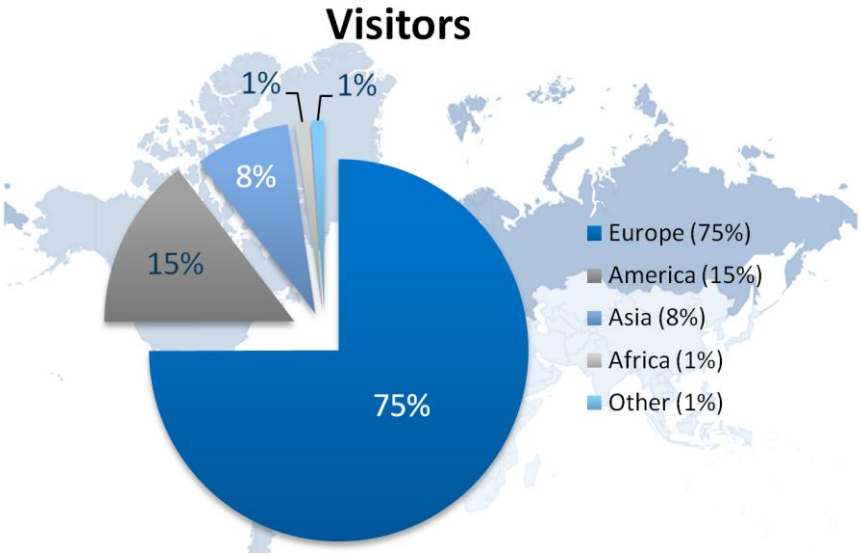


Figure 7: PRACTICE website statistic of the geographical distribution of visitor's location

It has to be also pointed out that the PRACTICE project was able to attract a considerable amount of new visitors, representing almost two thirds.

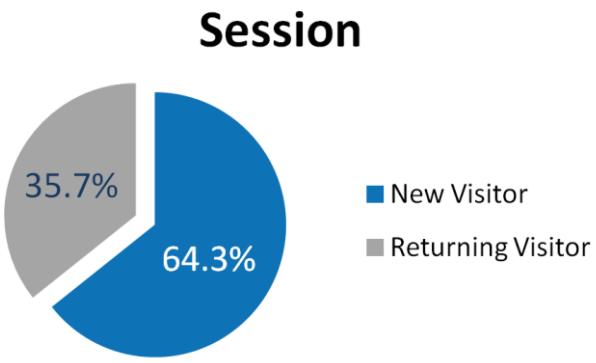


Figure 8: PRACTICE website statistic of the distribution of the type of the visitors

Considering the top downloaded documents during the whole October (M12) in the first project period, the PRACTICE Newsletter (Issue 2), which was published in July 2014, was the most frequently viewed/downloaded document of the PRACTICE website (140 hits), as shown in the following figure. Also gladly downloaded publication - 59 times - was a paper of the project partner *Katholieke Universiteit Leuven* with the title "Compact Ring-LWE Cryptoprocessor". Although the Announcement Letter was published last year right after the Kick-Off of PRACTICE, this document was downloaded 25 times during October 2014. This is closely followed by the PRACTICE Newsletter (Issue 1) with 24 hits and the Leaflet with 21 hits.

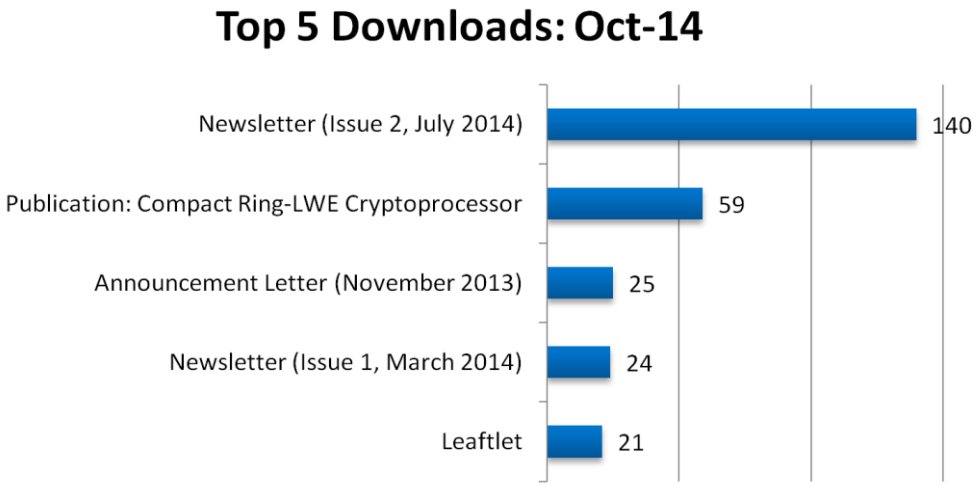


Figure 9: Statistic of the most frequently viewed/downloaded documents

1.2.3.2 Restricted Area of PRACTICE Website

Beside the public area, there is a password-protected area which is reserved for project participants in order to share project-internal data only (Figure 10). Thus only registered partners are able to enter it and can benefit from the options offered there, e.g.:

- Documentation and tutorials related to PRACTICE,
- Calendar for appointments and meetings,
- Mailing lists for reaching special mailing groups,

- Archives of the mailing list emails,
- SVN repository,
- iCal export of upcoming events

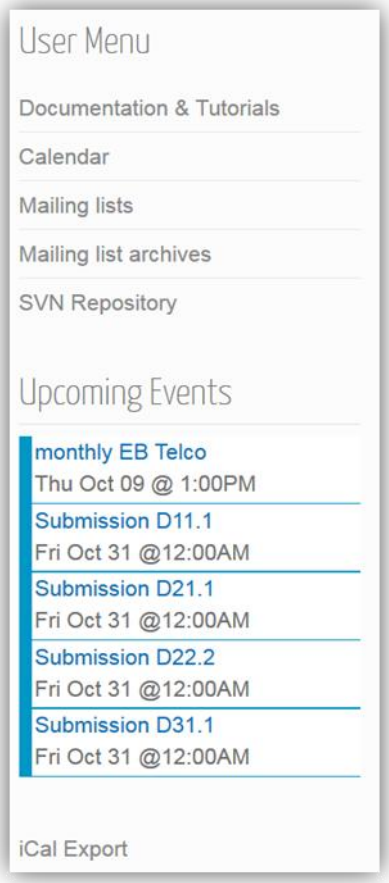


Figure 10: Content of the restricted area of the PRACTICE website

1.2.4 Presentation of the Project to the General Public

1.2.4.1 Web, Video, Flyers and Press Releases in Popular Press

All presentations to the general public are listed in an action overview list and are updated by the partners on a regularly basis. The project was presented to the general public in 5 different ways during the first project year.

Type of activities	Main leader	Title	Date			Place	Size of audience	Type and goal of the event	Countries addressed
			Day	Month	Year				
Press release	TEC, ALL partners	PRACTICE Announcement Letter	29	11	2013	Online	N/A	Press Release can be downloaded from PRACTICE website	International
Flyer	TEC, ALL partners	PRACTICE Leaflet	29	11	2013	Online	N/A	Official project leaflet can be downloaded from the PRACTICE website	International
Web	TEC, ALL partners	PRACTICE Newsletter Issue 1		3	2014	Online	N/A	Newsletter can be downloaded from PRACTICE website	International
Video	TEC	Application scenario animations		6	2014	Online	N/A	Videos can be downloaded from PRACTICE website	International
Web	TEC, ALL partners	PRACTICE Newsletter Issue 2		7	2014	Online	N/A	Newsletter can be downloaded from PRACTICE website	International

Table 4: Dissemination activities

1.2.4.2 Project Logo

For the improvement of its visibility, the PRACTICE project has adopted a project logo (Figure 11). The logo is used on all internal templates as well as on external dissemination tools.

Figure 11: PRACTICE logo

1.2.4.3 Project Announcement Letter

The intention of the PRACTICE Announcement Letter was to communicate the project start and ideas towards the general public. It was released in November 2013 giving a summary of the project addressed to non-specialist citizens and outlines what the project is about and how its planned results would matter for citizens and consumers. It can be found on the PRACTICE website following

http://www.practice-project.eu/downloads/announcement-letter/PRACTICE_Announcement-Letter_nov2013.pdf

1.2.4.4 Project Leaflet

The official PRACTICE leaflet is a four page informative and graphically appealing A4 flyer, highlighting the objectives and the work programme of PRACTICE (Figure 12). It can be and has already been used for distribution at conferences or certain other events in order to provide further visibility to the PRACTICE project. TEC was mainly responsible for the design of the leaflet and distributed it to all partners after finalisation. An electronic version of the leaflet is available on the PRACTICE website.

http://www.practice-project.eu/downloads/publications/leaflet/PRACTICE-leaflet.pdf

Figure 12: PRACTICE leaflet

1.2.4.5 Project Newsletters

In the first half year of the project (M05), a newsletter of the PRACTICE project was launched in order to address project related news (Figure 13). A second newsletter was published in July 2014 (M09) showing ongoing activities in the project (Figure 13). Furthermore, the newsletter offers current information and disseminates important events. The newsletters can be found on the PRACTICE website and is also posted via the PRACTICE Twitter and PRACTICE LinkedIn account to catch further public awareness. It is planned to publish newsletters in a regular basis, in order to keep external partners and the public updated.

Figure 13: PRACTICE newsletter issues 1 and 2

1.2.4.6 Social Media: PRACTICE Twitter Account and PRACTICE LinkedIn Group

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

Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". So far we have tweeted 17 entries and have 27 followers. The PRACTICE project is available on https://twitter.com/FP7_PRACTICE

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

1.2.4.7 Cooperation with Other Projects

As part of PRACTICE project management and dissemination activities, other projects in the same area have been identified. The PRACTICE project management team at TEC contacted coordinators of these PRACTICE-related projects and provided them with the most important information on the PRACTICE-project. The intention is to place the links to the websites of the related projects on the PRACTICE-website allowing interest groups to come across related projects when visiting our homepage as well as an exchange of experiences between the project consortia. - http://www.practice-project.eu/links

All cooperations with other projects are listed in an action overview list and have been updated by the partners on a regular basis. Currently 6 cooperations have been established during the first project year.

Actual/ planned date (dd.mm.yyyy)	Place	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)	PRACTICE partners involved
06.01.2014	Tallinn, Estonia	Meeting, explanation of secure computation capability, agreement on pilot application development	Estonian Tax and Customs Board	Estonia	CYBER
May 2014	Online	link related projects to our PRACTICE website	FP7 project CACE	international	all
May 2014	Online	link related projects to our PRACTICE website	FP6 project OpenTC	international	all
May 2014	Online	link related projects to our PRACTICE website	FP7 project UNIQUE	international	all
May 2014	Online	link related projects to our PRACTICE website	FP7 project TCLOUDS	international	All
03.06.14	Tallinn, Estonia	Presentation of a secure VAT fraud detecton system prototype	Estonian Tax and Customs Board	Estonia	CYBER

Table 5: List of cooperation with external organisations or other projects/programmes

Chapter 2 Standardisation

One important path to impact are the PRACTICE standardisation activities. The goal is to increase demand for our technologies and establish ourselves as a technology leader in the space of encrypted computation in the cloud. By introducing our concepts into standards we also create a favourable environment for later broad adoption of our results.

2.1 Standardisation Strategy in M01-M12

The goal of the PRACTICE project is to improve the privacy offered to actual end users. One of the main focus areas is to allow processing on encrypted data wherever possible. Unlike today's processing of clear data, this substantially decreases the risks of privacy and confidentiality exposures by leakage of sensitive or privacy invasive data.

The goal of our standardisation activities is to promote the PRACTICE approach. While the technology is still evolving, the focus of our first standardisation efforts where we participated was to promote privacy of cloud-based services in order to increase the commercial demand for the PRACTICE technologies.

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

2.1.1 Privacy Standardisation at the World-wide Web Consortium (W3C)

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

At this time, there are two key initiatives underway:

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

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

2.1.2 ISO/IEC JTC 1 SC 27

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

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

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

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

2.2 Standardisation Results in M01-M12

2.2.1 Privacy Standardisation at the World Wide Web Consortium

Matthias Schunter (INTEL) has acted as one of three co-chairs of the W3C Tracking Protection Group (http://www.w3.org/2011/tracking-protection/). In 2014, the W3C Do Not Track group has made substantial progress towards publishing a draft version of the standard. It has addressed hundreds of issues and provided drafts of two standards

Tracking Preference Expression (TPE): The first document of this working group is the "Tracking Preference Expression" proposal. This proposal defines a technical protocol between a browser and a web-site that implements the following functionalities:

- ***Transmit User Preference*:** If a user chooses not to be tracked, one part of the protocol (the DNT header) defines how a browser can tell a web-site that the user prefers not to be tracked.
- ***Transmit site Policy and Behaviour:*** The protocol allows a web-site to express the privacy-enhanced behaviour it plans to use when processing data from users who preferred not to be tracked.
- ***Negotiation:*** The protocol allows a site to ask a user to opt-in to tracking (so-called user-granted exceptions).

This document is now in the "last call" state, i.e. was published for comments. Currently, the working group is processing the comments received. The next step will be to call for implementations.

This standard is widely adopted. All major browsers (Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, Apple Safari) have implemented a tracking preference that allows their users to opt-out using this draft protocol.

Tracking Compliance Specification (TCS): The second document that is currently in " work in progress" state is the Tracking Compliance Specification. The goal of this document is to define how sites should process data that is collected while a user has been transmitting the "do not track" signal. This includes the following elements:

- ***Basic Behaviour:*** The document defines what tracking data may be collected, how long it may be retained, for what purposes it may be used, and with whom it may be shared.
- ***Exemptions:*** For certain well-defined cases, the standard allows sites to perform some tracking despite receiving do not track signals. One likely exemption is "Fraud Protection", i.e., if the data is protected (silo-ed and/or encrypted) and is only used for the fraud detection purpose, then this data may be collected.

The working group is still processing issues on this document. We expect a publication as a "last call" proposal in early 2015.

2.2.2 ISO/IEC JTC 1 SC 27

In January 2014, the PRACTICE project sent a Category C liaison request ISO/IEC Joint Technical Committee 1 (Information Technology) Sub-committee 27 (Information security techniques). The request was to form liaisons with Working Group 2 that works on cryptographic techniques and Working Group 5 that works on privacy and identity techniques.

Our goal with this is to disseminate both the cryptographic techniques and their privacy applications developed within PRACTICE.

To strengthen the chances of acceptance and acquaint ourselves with the relevant projects in SC 27, a PRACTICE representative participated at the ISO/IEC JTC 1 SC 27 meeting in Hong Kong to follow up on the liaison request and present the project. The presentations were successful, and a letter ballot was started.

In September 2014, our liaison requests were accepted and actual work was initiated. The first target standard to contribute to is ISO/IEC 19592 (Secret Sharing) parts 1 and 2. We also made contributions to the ISO/IEC 29151 (Code of Practice for PII Protection).

In October 2014, PRACTICE liaison office Dan Bogdanov participated in the SC 27 meeting in Mexico City to represent the PRACTICE comments. The majority of PRACTICE comments were accepted and PRACTICE results will be included in the next drafts of the standard.

The acceptance rates were as follows:

1) ISO/IEC 19592 Secret Sharing – Part 1: General. 2 comments, 2 accepted.
2) ISO/IEC 19592 Secret Sharing – Part 2: Fundamental mechanisms. 6 comments, 5 accepted, 1 editorial comment rejected.
3) ISO/IEC 29151 Code of Practice for PII Protection. 14 comments, 14 accepted, accepted with modifications or superseded by similar comments from other bodies.

2.3 Per-Partner Standardisation Plans for M13-M36

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

TEC: TEC, as coordinator, actively supports the standardisation activities of the consortium and provides assistance where needed and appropriate. Furthermore TEC is the interface between the Standardisation Institute and the partners.

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

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

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

UMIL: E. Damiani is chairing one of the working groups of the CEN workshop “Requirements and Recommendations for Assurance in Cloud Security (RACS)”. CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 33 European countries. CEN is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially

recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level. RACS intends to use the findings of several projects co-funded by the European Commission and provide a series of requirements and recommendations to tackle the challenges related to the assurance in the cloud. Goal of the CEN workshop is to embed the findings of several European projects and additional inputs from other WP participants into two CEN Workshop Agreements (CWAs). Liaisons with the activities of ISO/IEC/JTC SC 27/WG1 “IT Security Techniques” and ISO/IEC/JTC SC 38/WG3 “Distributed applications platforms and services”, involved in international standardization activities on cloud computing have been established and a series of meeting have been already planned before the end of 2014 and at the beginning of 2015.

Chapter 3 Exploitation

3.1 Introduction

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.

3.2 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 1 of the PRACTICE project.

Partner 1: Technikon Forschungs- und Planungsgesellschaft mbH (TEC) – Austria	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st 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 researches 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.
Initial report of exploitation activities	During the 1st period of the PRACTICE project, TEC has focused on the security specifications and requirements and transformed the use case scenarios into animated videos. The results have been shown to our customers and triggered their interest for the PRACTICE technology. Our competences have been increased as well as our external business reputation. Internally we started to investigate privacy shortcomings of our frequently used “cloned” doodle poll tool and we looked into the applicability of PRACTICE technology for a privacy enhanced poll tool and its potential future integration in our trusted knowledge suite.

Partner 2: SAP AG (SAP) – Germany	
Exploitation Plans according to Annex	**SAP** is a leading provider for enterprise solutions and also heavily invests in the vision of software-as-aservice. As such, SAP expects PRACTICE to

I	have a direct impact on its future product portfolio, impacting e.g. its supply chain management software and services in particular cross-organizational planning and execution. In addition to the concrete exploitation plans in the supply chain management software and services domain, the PRACTICE framework and architecture of an untrusted cloud service provider is also very relevant to many other of the software-as-a-service collaboration scenarios SAP and its customers are interested in, because of its generic applicability. The SAP Applied Research practice has been tasked with identifying technologies for the next-generation cloud platform, including platform-as-a-service offerings. The results of PRACTICE will be integrated with this platform and is likely to be piloting within SAP's existing cloud infrastructure. The on-demand (software-as-a-service) market is a key element for SAP's future and collaboration as pursued by PRACTICE is recognized as a key enabler of SAP's strategy. Several initiatives have been kicked off at executive level that could directly benefit from PRACTICE. SAP has recently shown its drive for software-as-a-service by several announcements of SAP board members Vishal Sikka and Jim Snabe at the SAP TechEd and Sapphire 2012 conferences. For the PRACTICE project SAP targets particularly the emerging platform-as-a-service platforms of the SAP portfolio. It will also put a strong focus on unique features of secure supply chain collaboration as a key differentiator enabled by PRACTICE, but use the PRACTICE secure cloud framework as a basis for other cloud application developments in the framework of the future cloud platform.
Updated exploitation plans after 1st project year including stakeholder	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 paving the road for projects like PRACTICE. 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. It is of main importance to create visibility, determine the product roadmap and involve the developers and development managers in the exploitation process. We therefore created the following updated exploitation plan for PRACTICE. 1st year: Create Awareness in the Development Organization. We will participate in developer conferences and hold management workshop in order to make the stakeholders aware of the on-going project. 2nd year: Create Demand and Roadmap. We will involve decision makers and pilot customers in order to create a roadmap for the productization of PRACTICE results. 3rd year: Initiate Transfer. We will create a detailed transfer plan and intend to hand over the developed code.
Initial report of exploitation activities	In the first year the plan was to create awareness. As such we participated in internal developer conferences, held meetings with internal stakeholders and ran in internal entrepreneurial competitions. Overall the results are as follows: • We held meetings with 12 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. • We won the 2nd place in the software development organization (P&I headed by Bernd Leukert) in the Hasso Plattner Founders' Award – the most prestigious SAP internal award with 100.000 EUR prize money. The selection among the 5 highest ranked contestants was made by Bernd Leukert himself.

Partner 3: Technische Universitaet Darmstadt, Intel Collaborative Research Institute for Secure Computing (TUDA) – Germany	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**TUDA** is one of the leading universities in Germany with a strong focus on engineering and computer science. Its department of computer science ranks among the best in Germany. In 2008, the TUDA, the Fraunhofer SIT and the Darmstadt University of Applied Sciences, have established the Center for Advanced Security Research Darmstadt (CASED), which is internationally recognized as one of the largest and most prestigious alliance for IT security within Europe. In this project TUDA analyses the existing secure computation techniques related to the group's competencies, builds complete specification of necessary applications and protocols, designs and implements those protocols and deploys them in the Cloud. Also they help to build the business model for collaboration services and assist in service implementation. Furthermore, they take part in the project management. TUDA will present PRACTICE in the following events/activities: • CROSSING Event, June 2015 in Darmstadt/Germany: The goal of the Collaborative Research Center CROSSING (https://www.crossing.tu-darmstadt.de/) is to provide cryptography-based security solutions enabling trust in new and next generation computing environments. The solutions will meet the efficiency and security requirements of the new environments and will have sound implementations. They will be easy to use for developers, administrators, and end users of IT, even if they are not cryptography experts. • European Privacy Research Day in Darmstadt/Germany • TUDA (Professor Sadeghi) will present a special session in DAC 2015 (Design Automation Conference) on Industrial Internet of Things and Cloud. • We will keep on presentation of PRACTICE to various companies, in order to draw attention of industry to the project. • TUDA will organize a Summer School in 2015 in order to present PRACTICE to the academia and students. We aim to enable application of PRACTICE outcomes in academic world.
Initial report of exploitation activities	During the first year of the project, TUDA has been continuously involved in several events, where PRACTICE project and its results were presented. TUDA published a few papers in renowned security conferences and organized workshop(s) and a summer school. PRACTICE goals and results were also presented to the audience of the invited talks given by TUDA representatives in high-profile events. The publications, talks, workshops and presentations can all be found in this document. We also presented PRACTICE to different companies such as Qualcomm.

Partner 4: Alexandra Institutte A/S (ALX) – Denmark	
Exploitation Plans according to Annex I	**ALX** is recognized by the Danish government as an advanced technology provider. As such, they are obliged to keep abreast with the state-of-the-art in a number of areas including security and cryptography. More importantly, ALX sees secure computation – in particular multi party computation (MPC) – as a strategic business area. It is working on projects leveraging MPC to realize solutions in diverse areas such as benchmarking, digital rights management, and privacy in relation to both public databases and location based services. ALX is a co-founder of Partisia (PAR) and has helped them to develop the Danish electricity auction site energiauktion.dk, hosted on Amazon Web Services and using MPC to ensure confidentiality. ALX aims

	to build on its experience with MPC to become a leading provider of software for secure computation solutions. This is in perfect alignment with the PRACTICE project, as it will help ALX to build state-of-the-art commercially leveraged software and as maintain its staff's competencies in the area.
Updated exploitation plans after 1st project year including stakeholder	In the second year of PRACTICE ALX plans to continue its exploitation activities as started in the first year. As described below this includes development of prototypes of applications using secure computation and a platform for secure computation. Furthermore, ALX plans to start work on implementing various protocols developed by the PRACTICE partners.
Initial report of exploitation activities	In the first year of PRACTICE ALX's activities towards our exploitation goals includes: Joint development of a platform for secure surveys using secure computation. Work on the development of a prototype for secure benchmarking of bank customers in collaboration with several small and medium sized Danish banks. Updating and extending ALX's internal software libraries for secure computation (the FRESCO framework). And initial work on a platform for secure computation to be delivered inside the PRACTICE project.

Partner 5: Arçelik A/S (ARC) – Turkey	
Exploitation Plans according to Annex I	**ARC** has 14 production plants in Turkey, Romania, Russia, South Africa and China, and provides products and services to its consumers in more than 100 countries. ARC has over 1400 suppliers worldwide, a significant fraction of those are SMEs. ARC's import and export logistics groups handles over 81000 shipments per year in which many data exchange transactions happens. This transaction volume doubles with the inclusion of inland shipments. These data is sensitive for Arçelik and its suppliers taking part in these transactions and it should be kept confidential. Thus, ARC will exploit PRACTICE's Security Service Platform (SERP) to share data with its suppliers securely and fast to increase its competitiveness. This platform will enable secure forecasting, planning and monitoring using modern Internet technologies in a more cost effective and high quality manner. ARC will inform all its suppliers and customers during bilateral meetings, company visits and trade shows about the potential outcome of the PRACTICE project to persuade them to benefit from PRACTICE's results. ARC will select and integrate a number of its suppliers for a demonstration and show this to its suppliers and interested Koç Holding companies to increase the deployment of PRACTICE results.
Updated exploitation plans after 1st project year including stakeholder	Arcelik is planning to present PRACTICE project at one of the Koc Technology Board meeting/event in 2015 showing potential outcome and exploitation possibilities to inform Koc Group of companies active in car manufacturing, energy, finance and agri-food sectors. Arcelik's suppliers will be also informed about the project progress during annual supply chain event in 2015. Finally, Arcelik is planning to show PRACTICE poster and distribute brochures at its stand in events, trade shows where Arçelik will participate throughout the 2nd year.
Initial report of exploitation activities	Arcelik has already shared 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 first year. PRACTICE project brochures were distributes at Arcelik stand or Arcelik's other project stands in a number of events during the first project year including ECFI-1 in Brussels, ECFI-2 in Munich, FIA Event in Athens, Innovation week in Izmir and Istanbul.The interested stand visitors have been informed about the project and potential outcomes during these events.

Partner 6: Bar Ilan University (BIU) – Israel	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**BIU** has a leading research group in efficient secure multi-party computation. The group develops and maintains the SCAPI open-source cryptographic library for secure multi-party computation, which is used by other projects around the world. The novel solutions developed in the PRACTICE project will be incorporated into this library. BIU plans to perform the following exploitation plans in year 2 of the project: • Present the technologies developed in the PRACTICE project in the 5th Bar Ilan Winter School on Cryptography which will be held on February 15-19, 2015. The school will have more than 150 participants who are experts and students who work on secure multi-party computation. • Incorporate technologies developed in PRACTICE into the SCAPI library, and publish the availability of these tools to current and potential users of the library. • Present the scientific results developed in the PRACTICE project in different leading academic conferences and seminars.
Initial report of exploitation activities	During the first year of the project, BIU performed the following exploitation activities: • The scientific results of the project were presented in different academic conferences, such as Crypto 2014 and the Usenix Security conference • Presentations of the project were given at different academic forums and at IBM Research. • The project was presented in the 4th Bar Ilan Winter School on Cryptography which was held on February 15-19, 2014. The school had about 140 participants. • Technologies developed in the PRACTICE project were incorporated into the SCAPI library.

Partner 7: Cybernetica AS (CYBER) – Estonia	
Exploitation Plans according to Annex I	**CYBER** has developed both prototypes and real-world applications based on secure computation technology, e.g. a secure financial data analysis system for the Estonian Association of Information Technology and Telecommunications. It plans to continue the development and sales of such systems. CYBER intends to license the platform for such systems, built around the secure computation application architecture developed within the PRACTICE project, and to offer application development and integration services. CYBER will also develop a platform-as-a-service cloud system that simplifies the deployment of secure computation technology. Companies requiring secure computation applications but lacking the resources to host the technology can rent cloud servers configured with a working secure database and application server. The novel tools deployed within PRACTICE will also allow the developers to create and generate applications without special cryptographic knowledge.
Updated exploitation plans after 1st project year including stakeholder	General explanation: Cybernetica is an ICT company with extensive history in bringing academic security technologies into the commercial domain. For example, Cybernetica has developed the Estonian ID card pilot project, digital signature legislation, timestamping technology, e-government bus technologies and internet voting techniques. Cybernetica plans to continue this series with the Sharemind secure computing technology. Cybernetica's exploitation plans within PRACTICE include the following

	activities. • Joint development of a privacy-preserving survey platform based on secure multi-party computation and its practical use in applications with real world stakeholders. • Launch of freely available open source Software Development Kit that will invite more users to the commercial Sharemind offerings from Cybernetica and other PRACTICE partners. • Launch of a Platform-as-a-Service cloud service that simplifies the deployment of Sharemind applications, increasing the uptake of the technology. • Development of pilot applications in the field of medicine in collaboration with real world stakeholders.
Initial report of exploitation activities	We will report the progress on each of the four areas. • The survey platform development has begun. The platform is functional. Cybernetica has conducted two employee satisfaction surveys internally to study the process and is currently negotiating the satisfaction survey in the Tartu city government in Estonia. • The first version of the Software Development Kit is launched on http://sharemind-sdk.github.io. We are in contact with its first users to gather feedback. • We are planning the first test deployments that will lead to the development of the cloud platform. • We have approached various stakeholders with collaboration proposals but have not yet fixed the project.

Partner 8: Julius-Maximilians Universitaet Wuerzburg (UWUERZ) – Germany	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**UWUERZ** will publish papers in scientific journals and take part in relevant conferences. Results from PRACTICE are also showcased during university lectures. Besides, various theses with related topics are supervised. All this creates awareness for the ideas and solutions developed by PRACTICE amongst an audience which soon is in the positions to decide whether their future employer should spend money for these ideas or not. Our research centres on collaboration approaches that protect the privacy of sensitive data and make supply chain collaboration secure, easier, and more efficient. Furthermore, UWUERZ will intensify the contact with other industrial partners which show interest in future results.
Initial report of exploitation activities	During the 1st period of the PRACTICE project, UWUERZ focused on finding mathematical planning models and determining other possible applications for PRACTICE results in various supply chain settings. Thereby, first working papers were drafted. Furthermore, a survey amongst various German and international companies was prepared to assess the relevance of secure collaboration for maintenance planning mainly in the plant construction and engineering sector. We presented the concept of secure maintenance planning using machine learning in a meeting with the innovation department of a big German aerospace MRO.

Partner 9: Intel GmbH (INTEL) – Germany	
Exploitation Plans according to Annex I	**INTEL** has 40+ years of experience of adapting foundational components in computing to the requirements of the computing ecosystem**,** Cloud computing and related server technologies have been focal areas for the technology development, and this experience has been extended to the idea of compute continuum between connected devices of various kind,

	where general principles, including security to the universe of devices and the cloud. Intel will leverage the achievements of the PRACTICE secure cloud framework in a variety of essential cloud and infrastructure related activities. A particular focus is to understand hardware requirements and extensions that will make the Intel platforms optimised for protecting confidential end-user data against cloud insider threats.
Updated exploitation plans after 1st project year including stakeholder	**INTEL** has 40+ years of experience of adapting foundational components in computing to the requirements of the computing ecosystem**,** Cloud computing and related server technologies have been focal areas for the technology development, and this experience has been extended to the idea of compute continuum between connected devices of various kind, where general principles, including security to the universe of devices and the cloud. We now put increased emphasis on low-end and IoT processors. Intel plans to exploit the PRACTICE secure cloud framework in a variety of essential cloud and infrastructure related activities. A particular focus is to understand hardware requirements and extensions that will make the Intel platforms optimised for protecting confidential end-user data against cloud insider threats. In this area, we will investigate how the results can be used to enhance privacy of data collection in IoT systems.
Initial report of exploitation activities	We conducted meetings and workshops in Intel where we presented results from PRACTICE: Our goal is to foster buy-in by our business units.

Partner 10: Katholieke Universiteit Leuven (KU LEUVEN) – Belgium	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**KU Leuven** The PRACTICE project will allow KU Leuven to expand her knowledge and expertise on secure data processing using multi party computation techniques. The prime interest of KU Leuven as an academic partner is to publish research results in high ranking international conferences and to earn reputation and publication credit points with conference contributions. An intended impact of these publications is that they will attract industry stakeholders and follow-up projects. Furthermore, the research and technology development will increase COSICs visibility and will improve education and teaching of students by incorporating recent research results in courses and seminars. In the second year we already foresee the following plans: • Our paper Efficient Software Implementation of Ring-LWE Encryption will be presented at the DATE 2015 conference. • We will again target to publish at the CHES conference which is one of the highest rated hardware security conferences. • We plan to integrate the software and hardware code into open source libraries built on top of the existing HeLib.
Initial report of exploitation activities	During the first year the results obtained in the PRACTICE project were exploited as follows: • Our paper on compact RLWE cryptocoprocessor was presented at CHES 2014 which is the leading conference on hardware security. The paper was also downloaded more than 50 times from the PRACTICE website. • Building on some of the technology in PRACTICE, we proposed several new projects, most of which received funding under the H2020 framework. Most notably the HEAT project (Homomorphic Encryption Applications and Technology) of which KU Leuven is the

	leader. A second related project that we are involved in is the WITDOM project (empoWeringprIvacy and securiTy in clouDenvirOnMents). As such the different projects will feed back into each other.

Partner 11: INESC PORTO – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC Porto) – Portugal	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**INESC PORTO** (currently INESC TEC) was created over 25 years ago to act as an interface between the academic world, the world of industry and services and the public administration in Information Technologies, Telecommunications and Electronics (ITT&E). INESC TEC brings together more than 800 collaborators, of which around 300 have PhDs (250 integrated PhDs in 600 researchers), forming a robust cluster with complementary skills, with notable international presence, and covering all stages of the knowledge production chain. In the PRACTICE project, INESC TEC will be actively involved in dissemination via scientific publications, participation in industrial events, and training activities. The knowledge and technology developed in PRACTICE will also be exploited in ongoing and future national and international projects, where cloud infrastructure is required to support applications with complex security requirements, namely in the area of Smart-Grids and Smart-Cities.
Initial report of exploitation activities	In the first year, the collaboration with PRACTICE partners has lead to the identification of a use case for verifiable computation in the area of smart metering, which has been pursued in parallel with a nationally funded project in the area of SmartGrids. This has lead to a publication in the IEEE Symposium on Security & Privacy, which will come out in 2015. A grant proposal titled SERECA: Secure and Resilient Cloud Architecture was also prepared during the first year and submitted for funding during the first year of PRACTICE; this can be seen as a spin-off of PRACTICE where INESC TEC and CYBER focus on the infrastructural aspects of cloud security. The SERECA application was selected for funding in 2015.

Partner 12: Aarhus Universitet (AU) – Denmark	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**AU** and its cryptography group has been focusing on MPC as a strategicallyimportant research area for at least 10 years. We have always believed that a combination of applied and basic research in the area is the most productive approach, and this aligns perfectly with what PRACTICE is doing. We intend to put the results from PRACTICE to good use in our ongoing collaboration with industry. We are, for instance, leaders of the CFEM centre, supported by the Danish strategic research council. Here we have several industrial partners and we apply MPC to build various prototype systems. One example is a system for financial benchmarking, where we can use MPC to protect confidential data that the involved parties would otherwise not get access to.
Initial report of exploitation activities	AU will exploit the output from PRACTICE in several ways: first, since AU was already doing research in MPC and will continue to do so after the project, the scientific results of PRACTICE will be very instrumental in helping us maintain our competitive advantage in relation to primarily US universities who are currently investing heavily in the area. In addition we will also benefit on the educational side, where the

	results of PRACTICE can be exploited in student projects both on the master and PhD level. Finally, AU has several working relationships with companies interested in various aspects of MPC, and the results of PRACTICE will clearly help us in continuing to be an interesting partner in industrial projects.

Partner 13: Technische Universiteit Eindhoven (TUE) – Netherlands	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**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.
Initial report of exploitation activities	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. Furthermore, we have broadened our research into secure multiparty computation, extending into several directions all connected to verifiability, resulting in several works (finished and in progress). Finally, we have worked on several prototypes, partly relying on VIFF and SCAPI. All these activities reinforce TUE's position as a center of expertise in secure multiparty computation.

Partner 14: University of Bristol (UNIVBRIS) – United Kingdom	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**UNIVBRIS** uses participation to the PRACTICE project to identify research areas that are relevant to the application of multiparty computation to real world problems. Solutions to such problems should lead to scientific output to be presented at workshops and conferences, which is our main goal. In addition, we expect that both the results of the project and the foundations on which they build will be presented at the training schools and workshops that we organize.
Initial report of exploitation activities	Results on verifiable computation, developed as part of PRACTICE, have been presented at CRYPTO'14. Ongoing work on primitives for verifiable computation will be published at PKC'15. Furthermore, results from the project will serve as basis of training for students at the school that PRACTICE will organize in September 2015.

Partner 15: Distretto Tecnologico Aerospaziale S.C. A R.L. (DTA) – Italy	
Exploitation Plans according to Annex I	**DTA** is a consortium of public and private players focused on research and development of innovation for the aerospace industry. Participating in research projects and leveraging knowledge, competences and results built through them in the local aerospace network is the objective of DTA staff. Italian aerospace industry, as well as DTA members, pushed by global competition, is stressing research and innovation programs aimed at improving supply chain-wide productivity and cost management. DTA will

	exploit PRACTICE's results in two areas: the management of confidential data in supply chains, and the introduction of cloud-based collaborative systems. In the global aerospace supply chain, data protection is a mandatory feature for any new system to be introduced. The results of PRACTICE enable DTA to help ist members (in particular: SMEs) to develop and deploy collaborative systems handling confidential data, to recognize their capability of protecting the confidentiality of sensitive data, and to measure the benefits brought by their usage in shared processes (like supply chain management and monitoring). As the first priority, DTA plans to apply PRACTICE approaches, methodologies and systems for collaborative supply chain management and monitoring into a selected supplier's community of Avio, to grasp the economic and procedural benefits.
Updated exploitation plans after 1st project year including stakeholder	**DTA**, the Apulian consortium of public and private aeronautic actors (SMEs, big aeronautic firms, Apulian Universities), has the mission to support industrial actors in pushing their innovation capabilities. With this aim, it creates collaboration opportunities connecting high knowledgeable people from academy and research organizations and experts from industry in order to face next industrial challenges. As security is a higher barrier toward effective cooperation into the local network as well as into global aeronautic supply chain, the objectives of the exploitation are diffusing awareness about latest technological opportunities and best practices, applying PRACTICE methodologies in other contexts and strengthening the security performance of the ICT systems developed or used by its members. Those activities were carried out through direct communication between DTA staff and representative of members. During these meetings, posters and brochures explaining the PRACTICE projects were presented, moreover in order to reach a more extended audience, brochures and poster in Italian language were developed. In the next period other industrial operators will be informed on the project methodologies and security results and on the competences developed by the project team, and a more targeted sensitization campaign will be carries out; it will be aimed at highlighting at interviewed people (industrial managers, collaborative process owners, …) about the data security level of their current practices (if the case a questionnaire will be administered).
Initial report of exploitation activities	During the first year, the DTA team presented and described the new security landscape in collaborative scenarios, the analysis and modelling methodologies developed in the PRACTICE project, and the results achieved to a number of industrial people belonging at different local and nation aeronautic firms, some of them are: GE Avio, AleniaAermacchi, Augustawesland, Finmeccanica, Enginsoft. A direct result of this diffused awareness on secure data management service provision toward aeronautic firms is the introduction of data risk and security analysis, in line with that applied into the PRACTICE project, in the research and development project aimed at preparing the cloud infrastructure for an aeronautic 'test bed'. The project is targeted at the airport of Grottaglie that was declared 'test bed for UAV – Unmanned Aerial Vehicles' few months ago. The project is currently under preparation. DTA presented PRACTICE project at the international CAE Conference, held in Verona (Italy) on 27th and 28th October 2014, through an informative stand point during. DTA had the opportunity to present project results at two different communities: the aeronautic one, as users of the technology and, the software (developers and) vendors operating in the aeronautic and mechanical industries, that need to take in consideration new security issues while introducing collaborative systems targeted at supply chain scenarios.

Partner 16: Università degli Studi di Milano (UMIL) – Italy	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**UMIL** is involved in a number of research activities and SESAR LAB, operating in the Department of Computer Science, is a respected player both in teaching and in research on cloud- and security-related issues. The exploitation plan for the results of PRACTICE project involves different activities. The research results obtained in the PRATICE project will allow UMIL and SESAR LAB to establish itself as a major player in the security and trustworthiness of ICT and cloud infrastructures, producing international publications on related journals and magazines, and participating to conferences and workshops focused on related topics. The results will also be exploited to start new educational courses at postgraduate level on cloud security and secure computation, and including some of the topics in the current courses, since UMIL hosts the first Italian BA and MA in computer security. The results of the project will also be used to develop UMIL activities at the doctoral level, since it is involved in a number of international cooperation initiatives, such as the French-Italian doctoral college on Secure Collaborative Knowledge Management co-organized with INSA. In addition, SESAR Lab at UMIL operates as a technology transfer center collaborating with several European industrial partners in the context of cloud computing and any possibility to explore commercialization of research products of the project, will be explored as well.
Initial report of exploitation activities	During the first year, research activities included in PRACTICE have been used in different contexts. Papers have been prepared and submitted for publication, and presentations have been given in official and/or informal workshops and invited talks, as well as in meeting with companies fostering potential collaborations.

Partner 17: Partisia (PAR) – Denmark	
Exploitation Plans according to Annex I	**PAR** is a Danish SME focusing solely on commercializing Secure Computing. It is founded and owned by most of the researchers behind [BCD+09] together with the Alexandra Institute (ALX). Initially the company focused solely on secure auctions for commodities like agricultural products and spectrum auctions (Partisia is a pre-qualified as auction provider for The Swedish and well as the Norwegian Post and Telecom Authority, and in 2012 provided software for a spectrum auction in Norway). PAR also delivered the auction platform for the Danish market place for electricity. PAR plans to generalise its cloud-based auction platform to a general cloud platform for secure computing, a goal which is tightly aligned with the goals of PRACTICE. The idea is to build components, which will make it possible for PAR's customers to build SaaS-solutions with a built-in high level of security irrespective of the security of the underlying cloud providers and the security efforts of the SaaS provider itself.
Updated exploitation plans after 1st project year including stakeholder	PAR's strategic focus and general exploitation plan remains the same. However, the realisation requires both business partners as well as investors, which may change the tactical implementation. An example of this is Sepior.com - a spinout from PAR since the initial exploitation plan. Sepior focus on cloud based "Key-Management-as-a-Service" that utilize MPC to control and distribute cryptographic keys in the cloud without trusting the individual cloud providers involved. The limitations on competitive activities imposed to PAR from this operation, do not influence PAR's continued focus on developing MPC services that ultimately may allow PAR's customers to build MPC based SaaS-solutions.

Initial report of exploitation activities	During the first year, PAR's exploitation activities have primarily focused on meetings with stakeholders about the two applications on MPC based surveys and benchmarking. A meeting with a Danish consultancy house focused intirely on surveys, confirmed that the "trustee function" (which we built into the software), is a large part of what they sell today. This may indicate that larger and well-established consultancy houses may see MPC based survey as a threath rather than an opportunity. Based on this initial insight, a list of potential collaborators is maintained and when the survey application is finished, further exploitation will be discussed with these potential business partners. Initial explotation activities concerning the next deliverable (D23.2) has been conducted as well. This has resulted in a sparring group that will follow and commenting the development. The sparring group consisting of the following potential endusers; two commercial Danish banks, one P2P lending site and one accountancy house. In more general terms, PAR has discussions about MPC based statistics with people involved in "big data". Here the initial focus is on automated trading systems based on MPC based statistics and auctions. PAR's experience with auctions and the PRACTICE applications in WP23 are aligned with this focus. However the outcome of these discussions are unclear at this stage. Finally, PAR has also directly and indirectly been represented at different conferences such as "Real world crypto" in 2014 and the conference "big data – big impact" in Denmark.

Partner 18: Georg-August-Universitaet Goettingen Stiftung oeffentlichen Rechts (UGOE) – Germany	
Exploitation Plans according to Annex I	No partner specific plans mentioned in Annex I
Updated exploitation plans after 1st project year including stakeholder	**UGOE:** UGOE will publish articles in scientific journals and take part in legal conferences. The results of research will be disseminated in possible conference proceedings. In addition the results of research may be published and elaborated further in articles in legal journals and reviews. Furthermore UGOE will contribute to dissemination activities of other project partners as far as they relate legal topics.
Initial report of exploitation activities	During the first year, UGOE's exploitation activities have focused on the collection and arrangement of materials (cases, articles, books) as a source for articles, reports and conference proceedings concerning legal problems and solutions regarding the project outcomes. An article regarding the importance of the element of "reference to persons" in the field of cloud computing has been published in Issue 6/2014 of PinG (Privacy in Germany). The work for another article has begun and is ongoing.

3.3 Joint Exploitation Strategies

In addition to the individual exploitation activities mentioned above, the partners performed common exploitation activities as well. The project website was exploitation-oriented upgraded and the first 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 Chapter 1.2.2. The partners also worked jointly on the use cases and identified corresponding business opportunities.

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

3.4 IPR Issues Identified in the PRACTICE Project

In the environment of international applied research projects with industrial partners such as PRACTICE, the careful handling of intellectual property rights (IPR) issues is of strategic importance. Within the PRACTICE project, many individuals of numerous organisations cooperate across national borders. In order to develop novel technologies, concepts or processes, exchanging information with other parties is a necessity. Furthermore, jointly creating new intellectual properties is common. Therefore confidentiality is a very important issue for participants in PRACTICE, from the project start-up phase of joint activities to the implementation phase and further to the exploitation of results.

All efforts related to IPR issues aim to create a favourable environment for respecting IPR. Without IPR protection the joint creativity of natural persons or legal bodies as well as the dissemination and exploitation of results would be highly restricted not to risk a substantial drain of knowledge. Intellectual property (IP) is an intangible asset and created as a result of intellectual creative effort of the human mind in relation to works of authorship and/or inventions. With the ownership of intangible assets certain legal exclusive property rights which are established by law or by contractual obligation are connected and maintain the control in relation to the protection of the interests of the creators by excluding these creations from public property. This means that right to permit or deny the use and exploitation of the creative work. So IPR provides a protection of the creations and inventions to the owners by preventing users from using or copying them without reservation or payment for a certain period of time.

Intellectual property can be classified into:

- Industrial property items like inventions which can be a product or a process providing new solutions for solving (technical) problems and which can be protected by registering a patent and
- Copyright items which provide exclusive rights to the creator to prohibit the authorized copying, adaptation and reproduction of its intellectual work.

The protection of the knowledge developed within PRACTICE is vital for each of the participants.

3.4.1 Prerequisites for the PRACTICE Project

The management of intellectual property in PRACTICE was already important at the project proposal set-up stage where the first development of appropriate ideas for the joint research activities and the assembling of the project consortium took place.

Even at this early stage, discussions and exchange of information between different people from institutions with different knowledge, background and interests was required and IPR issues needed to be discussed and integrated into the appropriate sections within the proposal.

Later on, the grant agreement (GA) represents a contract which establishes the beneficiaries' rights and obligations towards the European Community and towards each other. It contains a specific provision on confidentiality that defines the obligation and its term. Moreover, it also covers an intellectual property related section.

Furthermore, in order to guarantee a uniform approach by the PRACTICE participants, internal rules should be defined, including confidentiality clauses for the use of dissemination of results, which can be incorporated in the consortium agreement (CA).

In the present section, all stages and contracts, which are important IPR prerequisites for the project set-up will be briefly explained, with the focus on their implementation in the PRACTICE project.

3.4.2 Drafting of Proposals

In writing the project proposal for PRACTICE, the management of IPR was already outlined because the exchange of information between the partners in such an early stage is of certain risk. Although copyright allows some legal protection against unlawful copying of works, all parties should nevertheless only reveal any such information under terms of confidentiality in order to protect the contained ideas in a broader sense.

During the PRACTICE proposal drafting phase, it was laid down that the consortium agreement, as an outline contract between the partners, would define the rules and measures as well as the rights and duties for protecting the IP within the PRACTICE project. Through signing the consortium agreement and its confidentiality clauses the PRACTICE partners committed themselves to protecting the confidential information brought into or resulting from the PRACTICE project. Also plans for the use and protection of the results have been considered (more in “Consortium Agreement” chapter).

Additionally, the management structure has been set up with the protection of knowledge in mind, which foresees the permanent monitoring of IPR issues during the project.

3.4.3 Contracts

Within the PRACTICE project, two agreements have been prepared, which all partners had to sign in order to participate in the project: the grant agreement and the consortium agreement. Both of these agreements include IPR regulations for the project and therefore represent the contractual basis for IPR within PRACTICE.

3.4.3.1 Grant Agreement (GA)

The grant agreement is the contractual basis for the European Commission (EC) funded project PRACTICE, which is the principal agreement between the EC and the coordinator. This contract sets out in writing the key project details such as the parties involved, the scope, the duration and start date of the project, the reporting periods, the maximum financial contribution of the EC, the main contact data of the contracting parties as well as some specific issues.

It was clear to the project partners from the beginning that due diligence would be required with regard to confidentiality. Therefore they determined the level of confidentiality of information that would be provided in deliverables throughout the PRACTICE project when the work to be done in the project was defined and stated in Annex I to the GA.

3.4.3.2 Consortium Agreement (CA)

The consortium agreement is signed between the project participants of the consortium and implements the grant agreement, establishing provisions related mainly to consortium management, the distribution of the Community financial contribution and IP. The CA is a negotiated and agreed mandatory contract between the project partners, which has to be signed by all partners before the entry into force of the Grant Agreement. The legal requirements are singled out in the Grant Agreement but the details regarding the cooperation are given in a specific Consortium Agreement. The PRACTICE Consortium Agreement was signed by all partners in October 2013 and it sets out the internal

management guidelines for the consortium including established rules, structures and processes for handling IPR.

The CA includes guidelines for the project internal management of the cooperation by providing rules for the following issues:

- the parties' obligations for the implementation of the GA
- project internal organisation and project structure (project bodies and their functions, rights and duties, voting regulations)
- handling of commission payments (distribution of the funding by the coordinator)
- provisions about the ownership and licensing of intellectual property (e.g. foreground, publications, access rights, dissemination of results)
- handling of matters of liability and confidentiality
- procedures for settling internal disputes
- handling of defaults and remedies (exclusion/withdrawing)

Knowledge, or foreground[3], generated within the project will be protected by patent filing or publication in accordance with the consortium agreement that also represents an outline contract between the partners. The status of background[4] and side ground[5] brought in or developed in parallel is also covered by the CA. Amendments to the CA can be done on a per partner basis as the needs for knowledge and protection varies between the partners. With their signature of the CA, all partners agreed to the content of the binding Agreement.

Besides the general principles relating to access rights, the PRACTICE CA deals with clauses concerning access rights for affiliates as well as special provisions concerning access rights to software, standards and access rights for parties joining or leaving the project. Furthermore, the CA covers rules regarding the confidentiality period, exceptions, disclosure of confidential information in compliance with a court order and to the Commission as well as disclosure of confidential information to affiliates and it covers regulations regarding the disclosure of results to the public as well as the provided information to the EC.

3.4.4 Status Quo of the Project with Regard to IPR issues

On the basis of the above-mentioned contractual framework defined and agreed in the run-up to the project, the relevant intellectual property rights must be maintained during the project. Therefore, the management structure, workflows and tools are designed with the protection of knowledge in mind. The project management is responsible for the monitoring of IPR issues. All partners are obligated to report any protection of intellectual property to the project management.

New knowledge produced during the project belongs to the supplying partner and any commercial exploitation or public disclosure of new knowledge can only be done after the owner gives his consent. The decisions to patent any results belong to the owner; the other

[3] **Foreground** is understood to be tangible and intangible project results in terms of information, materials and knowledge generated inside the project. Foreground is principally owned by the partner who generated it; when the generation of the foreground is a joint process, it is - unless the partners do not agree on another solution - jointly owned by the participants.

[4] **Background** is understood to be information, knowledge and any IPR relevant to the project already held by the project partner before the accession to the EC Grant Agreement.

[5] **Sideground** is intellectual property created during a contract but which is not considered to be part of the contract.

partners must not interfere in this process. In case of jointly developed new knowledge the ownership needs to be agreed upon before any dissemination and/or exploitation.

The protection of knowledge, or Foreground generated within the project, is vital for each of the PRACTICE participants and is mainly realised by patent filing and/or publications.

The following subchapters should provide an insight regarding the current situation concerning different IPR issues within the PRACTICE project.

3.4.5 Patents

Until now, no patents were applied in reference to work generated within PRACTICE. However, it is a possibility that patents will emerge from results obtained in the PRACTICE project.

3.4.6 Copyrights

PRACTICE is generating copyrighted results. This includes source code, text, brochures, and web content. By default, everything developed by a partner is copyrighted by this partner, unless it is explicitly given a different status.

3.4.7 Violations

During the preparation phase of this document, all PRACTICE partners were asked whether they noticed any violations concerning IPR issues inside or outside of the project and none of them reported anything in this regard.

3.4.8 Partnerships with Other Projects/Partners outside PRACTICE Dealing with a Related Topic

Also in partnerships with other projects or partners, it is necessary to adhere to the IPR regulations and to share only ‘public’ PRACTICE-related information.

There have been several partnerships with other projects or partners dealing with a topic related to PRACTICE since, as reported in Section 1.2.4.7, many partners are involved in several other research or industrial projects. The collaboration activities have been guided from the common effort of each consortium partner, in order to enhance the impact of project’s results on other ongoing and/or upcoming projects.

3.5 Project Results

The following subchapter describes the development of project results (deliverables, reports and scientific publications) as well as the regulations of such results within the PRACTICE project.

3.5.1 Deliverables

All project participants are obliged to take care that the information provided in the deliverables and reports corresponds to the IPR regulations, especially when compiling public deliverables and reports.

In order to ensure that only public content is contained in public deliverables and that IPR rules have been considered, the PRACTICE consortium defined an internal review process for deliverables.

This process requires the approval of both the Project Management, and a reviewer external to the work package, before a deliverable is released. This ensures that the qualitative

targets are reached with regards to technical content, the objectives of the project and adherence to formal requirements established in the GAs and CAs.

Figure 14: Deliverables and publications process

The editor is responsible for appointing an external reviewer and sending a draft to the Project Management at least 21 days before the planned publication or delivery. This draft is also sent to the internal reviewer. A copy is similarly sent to owners of Intellectual Property related to the content. The reviewer and Project Management shall send their comments back to the editor within 5 days. The editor updates the deliverable within 5 days and sends it back to the Project Management for final approval.

The deliverable will be forwarded to the Coordinator who submits it to the Commission. The editor of any deliverable is by default the work package leader. It is the responsibility of the work package leader to ensure that the review form has been filled out correctly.

Review Form
for Project Management and Internal Reviewer

	Project Management:			Internal Reviewer:		
	Answer	Comments	Type*	Answer	Comments	Type*
1. Is the deliverable in accordance with						
(i) The Annex I - Description of the Work?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) the international State-of-the-Art?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
2. Is the quality of the deliverable in a status						
(i) which allows to send it to the EC?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) which needs improvement of the writing by the author of the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(iii) which needs further work by the partners responsible for the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a

Figure 15: Deliverable review form

3.5.2 Scientific Publications

For scientific publications, we use a publication mailing list to notify all partners about any future paper submission in order to prevent possible IPR conflicts. The basic rules are that the notification of any planned publication shall be given to the other Parties concerned at least 45 days before the publication in accordance with the GA II 30.3. According to the CA 4.4.1 a copy of any proposed publication in connection with or relating to the Project shall be sent to the Coordinator and by the Coordinator to the Parties at the earliest time possible. Any of the Parties may object to the publication within fifteen days after receipt of a copy of the proposed publication. The proposed publication shall not take place until the expiry of the period of fifteen days.

All publications and any other dissemination relating to the foreground shall include the following statement (GA II 30.4):

"The research leading to these results has received funding from the European Union Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-609611 (PRACTICE)."

Chapter 4 Internal and External Training

4.1 Introduction

Training and education is an important aspect of every successful project. It provides an opportunity to (i) *improve the skills of project members* – leading to a better understanding of the problem domain among members and thus a greater chance of producing better results, (ii) *enable knowledge sharing* – leading to better collaboration relationships and (iii) *disseminate project results* – enabling transparency of project activities and greater awareness of the problem domain and thus fostering further research.

Within the PRACTICE project, training and education will be facilitated to project members on the topics that relate to the activities of the project. To enable appreciation of the problems addressed within the project, the problems being addressed and the results obtained will be distributed in various forms, including articles, tutorials and demos, to a wider audience.

4.2 Training activities

PRACTICE consortium includes strong scientific and industrial partners, who are for the most part active in the research on topics related to the activities of the project. Anyway, a series of training initiatives have been planned in order to let members achieve an adequate level of skill within the project, broadening or improving the knowledge on fields or technique not directly included in their own research activities. These initiatives have been executed in different places and occasions, in order to reach the greatest number of people internal or external to the activities of PRACTICE.

4.2.1 Training at project meetings

In the first year, three 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. Meetings have been planned every six months (starting from the kick-off meeting in Darmstadt - November 2013, 1st technical meeting in Berlin - April 2014, 2nd technical meeting Istanbul – October 2014). Other regular meetings are planned in the next year and will provide place for further training sessions.

4.2.2 Training at schools

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

- BIU runs an annual winter school on cryptography. In Year 1 the school covered symmetric key cryptography, which is an essential tool for any cryptographic solutions. The school lasted for 4 days and had about 150 participants. Lecturers included Benny Applebaum (Tel-Aviv University), Eli Biham (Technion Institute of Technology), Orr Dunkelman (Haifa University), Iftach Haitner (Tel-Aviv University), Kenny Paterson (Royal Holloway, University of London) and Thomas Ristenpart (University of Wisconsin - Madison). All lectures were videotaped and are provided free of charge on the web.

- ALX/AU and PAR in collaboration with CTIC - Center for the Theory of Interactive Computation- have organized a workshop on the theory and practice of Secure Multiparty Computation, bringing together experts in all aspects of the subject. The first day of the workshop has been dedicated to tutorials covering the basic definitions, constructions and building blocks of secure computation. In the rest of the workshop, leading researchers in the field have presented their latest research results in secure computation. Lecturers included members of the consortium, and international expert as well.
- UNIVBRIS in collaboration with the Romanian Academy of Science and the University of Bucharest and the International Association for Cryptology Research (IACR) has organized a summer school on modern cryptography. The school has been held in Bucharest, Romania from 21 to 24 of July 2014. The aim of the school was to introduce the participants to the principles of modern cryptography as applied to the most basic primitives, being targeted to top undergraduate and graduate students, early career researchers, as well as security professionals. Some more advanced topics have been covered such as cryptography based on lattices and bilinear pairings. Lectures include Dario Catalano (University of Catania, Italy), Marc Fischlin (Darmstadt University, Germany), Vadim Lyubachevsky (Ecole Normale Superieure, France), Gregory Neven (IBM Research - Zurich, Switzerland), Tom Ristenpart (University of Wisconsin, U.S.), Tom Shrimpton (Portland University, U.S.)

4.2.3 Training provided elsewhere

In addition to the training shared at project meetings, some of the partners have had internal training and discussions restricted to the participants of subgroups formed to carry on the project's activities. Related materials that have been shared (via subversion) by various members have provided insights into cloud computing issues and a starting point for work on PRACTICE.

Work done in WP12 about the definition of application scenarios that can greatly benefit from secure computation technology has led to the production of short videos visualizing the basic idea behind the application scenarios and how they operate in an abstract way. The scenario animations are published on our PRACTICE website: www.practice-project.eu/applicationscenarios and can be used as training material to diffuse the fundamentals and the practical applications of secure computation.

4.3 Training planned

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

- Tutorial sessions during the project meetings;
- Workshops and schools: BIU2 has already planned to run a winter school on advances in practical multi-party computation, on February 15-19, 2015, The lecturers will be Ivan Damgård (Aarhus University), Yehuda Lindell (Bar-Ilan University), Claudio Orlandi(Aarhus University), Benny Pinkas (Bar-Ilan University), Abhi Shelat (University of Virginia) and Thomas Schneider (Technical University Darmstadt). The last day of the winter school will be a workshop in which advanced talks on this subject will be given. All lectures and talks will be videotaped and provided free of charged on the web.
- The preparation of a repository (to be included in the website) containing courses and tutorials, that can be offered for training and educational purposes, targeting academia and industry.