DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D6.3 – First Scientific & Research Impact Measurement

Due date of deliverable: 30 June 2019
Actual submission date: 31 May 2019

Grant agreement number: 780477
Start date of project: 1 January 2018
Revision 1.0

Lead contractor: Guardtime AS (GT)
Duration: 36 months

 Project funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open	X
CO = Confidential, restricted under conditions set out in the Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC	

D6.3

First Scientific & Research Impact Measurement

Editor
Björn Tackmann (IBM)

Contributors
Ahto Truu (GT)
Michele Ciampi (UEDIN)
Toon Segers (TUE)
Ivan Visconti (UNISA)
Karim Baghery (UT)
Sven Heiberg (SCCEIV)
Panos Louridas (GRNET)
Nikos Voutsinas (GUNET)
Nikos Karagiannidis (IOHK)

Reviewers
Name 1 (GT), Name 2 (GUNET)

31 May 2019
Revision 1.0

The work described in this document has been conducted within the project PRIViLEDGE, started in January 2018. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 780477.

Contents

Executive Summary

As a Research and Innovation Action, a clear focus of PRIViLEDGE is on strong research outcomes as well as their exploitation in the industry context. The present document analyses the impact of the research outcomes during the first half of the project duration.

The research output of PRIViLEDGE has started strong with overall 11 publications at scientific conferences, several of which are regarded as top-tier. Further additional presentations have been given at various venues. The earlier publications have started garnering citations, which indicates uptake by the academic community. To improve visibility within and interaction with the academic community, PRIViLEDGE has organized the PENCIL workshop affiliated with this year's Eurocrypt conference. The workshop featured a dense program of high-quality publications; it was the largest workshop at this year's Eurocrypt conference.

Use of research results in toolkits and prototypes of project partners, as well as their use in further activities, is one of the main focus points of PRIViLEDGE. Partners have updated their exploitation reports and plans, providing more concrete measures toward the use of the results.

1 Introduction

The scientific results are the centrepiece of PRIViLEDGE. They inform and influence the design of the toolkits and prototypes, and thereby steer the future products and services of the industry partners. They are taken up by the university partners in their teaching activities and in follow-up research performed at their institutes, shaping the material taught to the upcoming student generations. But they also serve as beacons for PRIViLEDGE, making the project and its partners more widely known in their communities.

The purpose of Deliverable 6.3, "First Scientific & Research Impact Measurement" is the analysis of the impact that the research performed within PRIViLEDGE has generated in the first 18 months of the project. As different types of research results generate impact in different, complementary ways, we consider a broad set of criteria including:

- Presentations of research results at venues with different audiences such as academic, business, governmental, or general public.
- Uptake by the academic community through citations and follow-up work.
- Concrete research results applied in the development of products or services of PRIViLEDGE partners, in open-source projects, or in standardisation efforts.
- Use of research results in contacts with clients and partners from different domains, such as industry or government.
- Set up of new collaborations in which the publicity through PRIViLEDGE or the research results obtained in the project was instrumental.

The impact of research results generated within a project does not materialise linearly over the project duration. For one, research results first have to be generated and published; this takes time. Even more: measurable impact often only occurs after the next iteration, that is, when follow-up papers have been published, or when a software project has released the next version that includes a new technology. We therefore highlight that the measurable numbers and items are expected to grow rapidly throughout the project, as the amount of exploitable results increases further over the project duration, and furthermore results from the first project period had more time to generate impact.

The research results generated by the partners are listed in Section 2. The list includes research papers (published, preprints, and unpublished drafts) as well as presentations that do not directly link to any of the papers. Section 3 then begins by providing an analysis of the impact that was generated by each of these results. As discussed above, we understand *impact* broadly and list different metrics or facts as appropriate. The section also discusses the "less tangible" impact, such as in setting up new collaborations or using the results in discussions or workshops with existing or new partners or clients.

Exploitation of research results by project partners is one key route toward generating impact. We therefore provide in Section 4 statements on exploitation measures taken so far by the project partners as well as updated exploitation plans with more concrete details in comparison with Deliverable 5.3. Section 5 discusses the impact up to M18 in view of the remaining project duration.

2 Scientific & research results

The project has produced a list of research results that have been published and/or presented at different venues and events. This section contains a list of results produced in the project, irrespective of their type. More specific analyses with respect to different types of impact are then given in Section 3.

[ABL+19a] Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, Janno Siim, and Michal Zajac. DL-extractable UC-commitment schemes. In Robert Deng and Moti Yung, editors, *ACNS*, volume 11464 of *LNCS*, pages 385–405. Springer, 2019.

[ABL+19b] Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, Janno Siim, and Michal Zajac. UC-secure CRS generation for SNARKs. In Johannes Buchmann, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Africacrypt*, LNCS. Springer, 2019.

[ACD+19] Elli Androulaki, Jan Camenisch, Angelo De Caro, Maria Dubovitskaya, Kaoutar Elkhiyaoui, and Björn Tackmann. Privacy-preserving auditable token payments in a permissioned blockchain system. In submission, May 2019.

[ACDK18] Elli Androulaki, Christian Cachin, Angelo De Caro, and Eleftherios Kokoris-Kogias. Channels: Horizontal scaling and confidentiality on permissioned blockchains. In Javier Lopez, Jianying Zhou, and Miguel Soriano, editors, *European Symposium on Research in Computer Security*, volume 11098 of *LNCS*, pages 111–131. Springer, 2018.

[ACKZ19] Aydin Abadi, Michele Ciampi, Aggelos Kiayias, and Vassilis Zikas. Timed signatures and zero-knowledge proofs –timestamping in the blockchain era–. In preparation, May 2019.

[ALSZ18] Behzad Abdolmaleki, Helger Lipmaa, Janno Siim, and Michal Zajac. On QA-NIZK in the BPK model. Cryptology eprint archive, report 2018/877, September 2018.

[Bag19] Karim Baghery. On the efficiency of privacy-preserving smart contract systems. In Johannes Buchmann, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Africacrypt*, LNCS. Springer, 2019.

[BCH+19] Christian Badertscher, Ran Canetti, Julia Hesse, Björn Tackmann, and Vassilis Zikas. Universal composition with global subroutines: Capturing global setup within plain UC. In submission, May 2019.

[BGK+18] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *CCS*. ACM, 2018.

[BJOV18] Saikrishna Badrinarayanan, Abhishek Jain, Rafail Ostrovsky, and Ivan Visconti. Non-interactive secure computation from one-way functions. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT*, volume 11274 of *LNCS*, pages 118–138. Springer, 2018.

[CCG+19] Arka Rai Choudhuri, Michele Ciampi, Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. Cryptology eprint archive, report 2019/216, February 2019.

[CDT19] Jan Camenisch, Manu Drijvers, and Björn Tackmann. Multi-protocol UC and its use for building modular and efficient protocols. Cryptology eprint archive, report 2019/065, January 2019.

[CO18] Michele Ciampi and Claudio Orlandi. Combining private set-intersection with secure two-party computation. In Dario Catalano and Roberto De Prisco, editors, *International Conference on Security and Cryptography for Networks*, volume 11035 of *LNCS*, pages 464–482. Springer, 2018.

[CT19] Christian Cachin and Björn Tackmann. Asymmetric distributed trust. In submission, May 2019.

[CV19] Michele Ciampi and Ivan Visconti. From Sigma-protocols to efficient NIZK without programmable random oracles. In preparation, 2019.

[GK18] Juan A. Garay and Aggelos Kiayias. SoK: A consensus taxonomy in the blockchain era. Cryptology eprint archive, report 2018/754, August 2018.

[GKZ19] Peter Gaži, Aggelos Kiayias, and Dionysis Zindros. Proof-of-stake sidechains. In *IEEE Symposium on Security and Privacy*. IEEE, 2019.

[HKSW18] Sven Heiberg, Ivo Kubjas, Janno Siim, and Jan Willemson. On trade-offs of applying block chains for electronic voting bulletin boards. In *E-Vote ID*. Tallinna Tehnikaülikooli Raamatukogu Digikogu, 2018.

[KKLS18] Aggelos Kiayias, Annabel Kuldmaa, Helger Lipmaa, and Janno Siim. On the security properties of e-voting bulletin boards. In Dario Catalano and Roberto De Prisco, editors, *International Conference on Security and Cryptography for Networks*, volume 11035 of *LNCS*, pages 505–523. Springer, 2018.

[KR18] Aggelos Kiayias and Alexander Russell. Ouroboros-BFT: A simple Byzantine fault tolerant consensus protocol. Cryptology eprint archive, report 2018/1049, October 2018.

[KZ18] Aggelos Kiayias and Dionysis Zindros. Proof-of-work sidechains. Cryptology eprint archive, report 2018/1048, October 2018.

[Lip19a] Helger Lipmaa. Key-and-argument-updatable QA-NIZKs. Cryptology eprint archive, report 2019/333, March 2019.

[Lip19b] Helger Lipmaa. Simple yet efficient knowledge-sound and non-black-box any-simulation-extractable ZK-SNARKs. Cryptology eprint archive, report 2019/612, May 2019.

[SSV19a] Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Publicly verifiable argument systems through generic blockchains. Talk at DLT workshop, 2019.

[SSV19b] Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Publicly verifiable proofs from blockchains. In Dongdai Lin and Kazue Sako, editors, *IACR International Workshop on Public Key Cryptography*, volume 11442 of *LNCS*, pages 374–401. Springer, 2019.

[SSV19c] Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Publicly verifiable proofs from blockchains and the attacks of the clones in proof-of-stake blockchains. In submission, May 2019.

[SV19] Luisa Siniscalchi and Ivan Visconti. On deleting data from a blockchain. Talk at DLT workshop, 2019.

3 Impact measurement

This section contains three different parts that correspond to different paths along which the project has created impact. The first and most obvious path is through academic publications and their uptake by the academic and industry communities. In Section 3.1, we analyze the results listed in Section 2 with respect to their impact in different communities. Section 3.2 then focuses on the first workshop organized by PRIViLEDGE, the workshop on *Privacy Enhancing Cryptography in Ledgers (PENCIL)* that took place in May 2019 in Darmstadt, Germany. Finally, Section 3.3 summarizes how participation in PRIViLEDGE has further benefitted the parties, such as through involvement in new partnerships, or the use of project results in other activities.

3.1 Publications and other concrete results

The most objectively measurable impact of project research is through academic publications and their uptake by the academic community. This section analyzes the impact of the research results listed in Section 2.

Paper	Partners	Type of result	Conference	Deliverable
[ACDK18]	IBM	Published paper	ESORICS	
[BGK+18]	UEDIN, IOHK	Published paper	ACM CCS	
[BJOV18]	UNISA	Published paper	ASIACRYPT	
[CO18]	UEDIN	Published paper	SCN	
[HKSW18]	SCCEIV, UT	Published paper	E-Vote ID	
[KKLS18]	SCCEIV, UEDIN, UT	Published paper	SCN	
[ABL+19a]	UT	Published paper	ACNS	
[ABL+19b]	UT	Published paper	Africacrypt	
[Bag19]	UT	Published paper	Africacrypt	
[GKZ19]	UEDIN, IOHK	Published paper	IEEE S&P	W3.2
[SSV19b]	UNISA	Published paper	PKC	D2.2
[ALSZ18]	UT	Preprint		
[GK18]	UEDIN	Preprint		D3.1
[KZ18]	UEDIN, IOHK	Preprint		
[KR18]	UEDIN, IOHK	Preprint		
[CCG+19]	UEDIN	Preprint		
[CDT19]	IBM	Preprint		
[Lip19a]	UT	Preprint		
[Lip19b]	UT	Preprint		
[ACD+19]	IBM	Unpublished draft		D2.2
[ACKZ19]	UEDIN	Unpublished draft		D2.2
[BCH+19]	IBM, UEDIN	Unpublished draft		
[CT19]	IBM	Unpublished draft		W3.2
[CV19]	UEDIN	Unpublished draft		
[SSV19c]	UNISA	Unpublished draft		W3.2

Table 1: List of research papers. The table emphasizes collaboration among research partners as well as the use of results from research papers in project deliverables.

Publications, Collaboration, and Deliverables. While the list in Section 2 list all research results independently of their type, Table 1 lists the publications ordered by their current state. The top part of the table lists 11 papers that have been published in different scientific venues. In particular, these venues include those specifically targeted by the project (according to the project proposal) such as ESORICS, ACM CCS, ASIACRYPT, IEEE S&P, PKC. The mid part of the table lists 8 papers that are currently available on preprint servers and are in different stages toward publication. Finally, the lower part of the paper lists 6 papers that are currently not available in public but have been submitted to conferences or covered in presentations given by members of PRIViLEDGE.

The table shows significant collaboration between research partners in generating research publications. Overall, 7 out of 25 papers include authors from more than one PRIViLEDGE partner. Finally, results from 7 papers have already been used in different deliverables of the project. Among those paper, [GK18] is a systematization-of-knowledge paper on research on consensus protocols, featured in Deliverable 3.1. Deliverable 2.2, *Definitions and Notions of Privacy-Enhancing Cryptographic Primitives for Ledgers*, contains material from 3 research papers, and Work Document 3.2, which is currently work in progress and will eventually feed into Deliverable 3.2, will also contain material from 3 papers.

Presentations of research results. Presentations of PRIViLEDGE research results are listed in Table 2. As indicated in the table, and consistent with the proposal, the early phase of PRIViLEDGE focuses on research

Paper	Presentation	Type of venue	Audience
[ACDK18]	ESORICS 2018	Academic, security	~ 100
[BGK+18]	ACM CCS 2018	Academic, security	~ 500
[BJOV18]	ASIACRYPT 2018	Academic, cryptography	~ 300
[CO18]	SCN 2018	Academic, cryptography	~ 100
[HKSW18]	E-Vote ID 2018	Academic, e-voting	~ 100
[KKLS18]	SCN 2018	Academic, cryptography	~ 100
[ABL+19a]	ACNS 2019	Academic, cryptography	~ 120
[ABL+19b]	Africacrypt 2019	Academic, cryptography	~ 100
[Bag19]	Africacrypt 2019	Academic, cryptography	~ 100
[ALSZ18]	Estonian-Latvian Theory Days	Academic, theory	~ 50
[ALSZ18]	Simula UiB	Academic, cryptography	~ 20
[CDT19]	Dagstuhl seminar, 2019	Academic, theory	~ 40
[GKZ19]	IEEE S&P 2019	Academic, security	~ 500
[KKLS18]	Estonian-Latvian Theory Days	Academic, theory	~ 50
[SSV19a]	DLT 2019	Academic, cybersecurity	~ 70
[SSV19b]	PKC 2019	Academic, cryptography	~ 110
[SV19]	DLT 2019	Academic, cybersecurity	~ 70
[ACKZ19]	PENCIL	Academic, DLT	~ 120
[ALSZ18]	PENCIL	Academic, DLT	~ 120
[CT19]	PENCIL	Academic, DLT	~ 120
[GK18]	PENCIL	Academic, DLT	~ 120
[SSV19c]	PENCIL	Academic, DLT	~ 120

Table 2: Public presentation of results.

results and their dissemination within the academic community. Consequently, the presentations in this phase also focused on the academic community.

The table shows that the venues cover a broad range, both in terms of size and in terms of topics. Some venues cover broad areas of security research, such as ACM CCS, IEEE S&P, or ESORICS, whereas other venues are clearly focused on cryptography such as PKC or ASIACRYPT, and again other venues are targeted as specific use cases, in this case e-voting, in the case of E-Vote ID. Likewise, while conferences like ACM CCS, IEEE S&P, or ESORICS allow to reach a large community at the same time, more focused events such as the Dagstuhl seminar of the Estonian-Latvian Theory Days allow to discuss specific results in more detail with a focused set of participants.

The PENCIL workshop, covered in the lower part of the table, plays a special role as it had the clear vision to promote PRIViLEDGE within the scientific community. In total, 5 of the presentations given at the workshop explicitly promoted research results of PRIViLEDGE. This workshop will be further covered in Section 3.2.

Citations and follow-up work. Citation counts are an often debated and criticised but still important measure of impact for scientific work. Needless to say, absolute counts at this stage of the project cannot be high, as the research results first had to be produced and published, before subsequent research could build on the results. Therefore, we suggest to view the data in Table 3 only as a first indication for (un)successful uptake of certain results, and not (yet) as an estimate toward expected future impact of individual papers.

As expected, papers first published later than October 2018 did not yet have enough time to be picked up by the broader research community, although some of them have influenced further research by PRIViLEDGE partners and received first citations through this. The papers first published between July and October 2018 started collecting first citations. The paper on Ouroboros Genesis [BGK+18], an improved version of the Ouroboros

Paper	Publication	Presented	Citations	Follow-up
[KKLS18]	July 2018	✓	4	
[CO18]	July 2018	✓	5	
[GK18]	August 2018	✓	6	
[ACDK18]	September 2018	✓	7	Informs discussions on cross-channel transactions in Hyperledger Fabric
[ALSZ18]	September 2018	✓	1	
[KZ18]	October 2018		4	Extended in [GKZ19]
[BGK+18]	October 2018	✓	15	Subsequent research by UEDIN, IOHK
[KR18]	October 2018		5	
[HKSW18]	October 2018	✓	3	
[BJOV18]	December 2018	✓	–	
[CDT19]	January 2019	✓	–	Used in [ACD+19]
[CCG+19]	February 2019		–	
[Lip19a]	March 2019		–	
[Lip19b]	March 2019		–	
[SSV19b]	April 2019	✓	–	Subsequent research by UNISA
[GKZ19]	May 2019	✓	3	
[ABL+19a]	June 2019	✓	1	Used in [ABL+19b]
[ABL+19b]	July 2019		–	
[Bag19]	July 2019		–	

Table 3: Citations and follow-up work. Numbers are from Google Scholar.

Praos proof-of-stake consensus protocol which is co-authored by authors from IOHK and UEDIN, has already spawned significant community interest. The state for most other papers from this time range is also promising, although as stated above, the absolute numbers should be interpreted with care.

3.2 Workshop PENCIL

The project organised the workshop on "**P**rivacy **En**hancing **C**ryptography **i**n **L**edgers (PENCIL)"[1] on May 18, 2019, in Darmstadt, Germany, as an affiliated event of the conference Eurocrypt 2019[2]. According to the project proposal, the workshop had two major objectives:

- present research results from PRIViLEDGE, and
- to engage in dialogue with the research community and ignite further academic work.

In order to achieve both objectives and attract many people from the academic community, the workshop was set up to consist of three parts:

- Presentation of research results from PRIViLEDGE,
- three invited presentations by widely-known experts,
- contributed presentations from the research community on relevant and timely topics.

The workshop had approximately 120 participants, making it the largest affiliated event of Eurocrypt 2019. After the workshop, we received positive feedback from different parts of the community, both on individual presentations and on the organization of the workshop as a whole.

[1] https://priviledge-project.eu/pencil
[2] https://eurocrypt.iacr.org/2019/

Presentation of research results from PRIViLEDGE. The schedule contained 5 presentations from PRIViLEDGE (and one invited talk that also covered material developed in the project), increasing the visibility of these results in the scientific community:

- *Asymmetric distributed trust* by Björn Tackmann (IBM) covered work from WP3 on protocols in settings in which parties have diverse and subjective trust assumptions about the system [CT19].
- *Publicly verifiable proofs from blockchains and the attack of the clones in proof-of-stake blockchains* by Luisa Siniscalchi (UNISA) covered work from WP2 on cryptographic proof systems that make use of distributed ledgers in the generation of proofs, which can then be verified non-interactively, as well as work from WP3 on attacks on proof-of-stake consensus protocols [SSV19c].
- *Timed signatures and zero-knowledge proofs — timestamping in the blockchain era* by Michele Ciampi (UEDIN) covered work from WP2 on using distributed ledgers for binding the generation of signatures and zero knowledge proofs to a certain time epoch [ACKZ19].
- *On QA-NIZK in the BPK model* by Behzad Abdolmaleki (UT) covered work from WP2 on reducing the trust assumptions of non-interactive zero-knowledge proof systems [ALSZ18].
- *Verifiable MPC and DLT* by Toon Segers (TUE) provided an outline of the work that TUE performs on the connection between MPC and TUE as part of PRIViLEDGE, as outlined in Deliverable 3.1.

Invited presentations. Three invited presentations were given at the workshop, by renowned experts of their areas.

- *A consensus taxonomy in the blockchain era* by Prof. Juan Garay (Texas A&M University) covered the milestones of consensus research from the last 40 years, starting with feasibility results for the traditional setting, through practical protocols, to the current *ledger consensus* type of protocol. The talk was based on joint research with Prof. Aggelos Kiayias, and part of the material was in PRIViLEDGE Deliverable 3.1.
- *A tale of a blockchain startup* by Mateusz Tilewski (Concordium) described the history of Concordium and their collaboration with Aarhus University and other academic institution, focusing on the tensions between open-science peer-reviewed research that builds the foundation of the company's products, and the need to still keep a competitive advantage in the market.
- *Why should I trust that?* by Jens Groth (DFINITY) gave a broad perspective on non-interactive cryptographic proof systems, and carved out the explicit and implicit trust assumptions that are required by the use of those proof systems in distributed ledger technologies.

Submitted presentations. The workshop also featured a series of presentations submitted by external researchers. Overall, we received 23 submissions, which were thoroughly reviewed by the program committee consisting of representatives from PRIViLEDGE as well as external researchers. 10 of the publications were chosen to be presented; 8 presentations were finally given at the workshop:

- *Afgjort – A semi-synchronous finality layer for blockchains* by Daniel Tschudi (Aarhus University) presented a consensus protocol that is a hybrid between a proof-of-stake ledger consensus derived from Ouroboros Praos and a "voting-type" protocol for achieving finality.
- *Pixel: Multi-signatures for consensus* by Hoeteck Wee (Algorand) presented a new signature scheme that combines multiple properties such as message aggregation, public-key aggregation, and forward secrecy.

- *A framework for anonymous lottery-based protocols in the proof-of-stake setting* by Varun Rajeev Madathil (North Carolina State University) presented a version of the Algorand protocol that allows parties to keep their stake secret.
- *Fully homomorphic NIZK and NIWI proofs* by Apoorvaa Deshpande (Brown University) introduced homomorphism for non-interacting proofs, that is, proofs for two statements can be combined (e.g. via *and* or *or*) and a proof of the composite statement can be obtained even without knowledge of any possibly necessary secret inputs.
- *Zether: Towards privacy in a smart-contract world* by Benedikt Bünz (Stanford University) presented a privacy-preserving token system based entirely on Ethereum smart contracts.
- *Bootstrapping online trust: Timeline activity proofs over public ledgers* by Mark Manulis (University of Surrey) argued that timeline activity on social computing sites are increasingly used as a method for verification of real users, and showed how distributed ledgers can help to build secure protocols for this purpose.
- *Quisquis: A new design for anonymous cryptocurrencies* by Prastudy Fauzi (Aarhus University) presented a privacy-preserving token mechanism that builds on a mix-in architecture (similarly to Monero) but in which the contents of transactions is hidden (similarly to ZCash).
- *Universally composable and privacy-preserving audit logs using bulletin board* by Anna Kaplan (TU Munich) showed how audit logs can be kept on a distributed ledger, while allowing for fine-grained permissioned auditing.

3.3 Collaborations of partners

As expected, participation in PRIViLEDGE has lead to strong collaboration between the partners of the project. In particular, each use case partner has been assigned explicitly to one or two academic partners in order to guide the research from a use-case perspective, and the use-case solution from a research perspective. This already lead to collaboration between partners that had never worked together prior to PRIViLEDGE.

Furthermore, several partners have reported collaborations that have been spawned directly or indirectly through their participation in PRIViLEDGE. IBM is now actively collaborating with University of Berne on research on consensus algorithms. Presentation of research work at a Dagstuhl workshop has also lead to a joint paper project with researchers from UEDIN, University of Rochester, Boston University, University College London, North Carolina State University, and the Karlsruhe Institute of Technology.

UNISA is collaborating with Maciej Obremski (National University of Singapore) on randomness extraction from blockchains, with Daniele Venturi (La Sapienza University of Rome) on securing smart contracts. Ivan Visconti (UNISA) became a member of the Center for Secure Distributed Ledgers and Contracts (TU Darmstadt).

4 Updated exploitation plans

4.1 Guardtime AS

4.1.1 Guardtime PRIViLEDGE goals

Guardtime's core technology is the KSI blockchain. Due to its off-chain transaction model, it already has very strong privacy guarantees, but does not provide any data sharing facilities. At the other end of the spectrum, represented by Bitcoin among others, all data is completely public. Guardtime's main interest in PRIViLEDGE is finding a middle ground between these extremes, as data sharing in controlled fashion is required in many business applications.

In theory, several cryptographic solutions such as homomorphic encryption, zero-knowledge proofs, and authenticated data structures could provide more controlled access in verifiable manner. In particular, zero-knowledge proofs seem attractive, as they would allow sharing verifiable claims about data without exposing the data itself. However, currently available cryptographic solutions tend to have too high overhead for practical deployment. New primitives and protocols developed in PRIViLEDGE could move these techniques into commercial viability.

4.1.2 Commercialisation

In the nearest term, Guardtime expects the PRIViLEDGE outcomes to strengthen its offerings in the health insurance sector, which is one of the demonstration use-cases in the project. In particular, the ability to provide verifiable reports on healthcare outcomes without disclosing the underlying patient records would be key in enabling wider use of outcome-based contracting in the sector. However, the cryptographic techniques developed in PRIViLEDGE for those goals in the health insurance use-case should be universal and thus applicable also in products and services for other verticals, most notably in the financial sector, in future developments.

In the medium term, the improved cryptographic tools developed in PRIViLEDGE are expected to bolster Guardtime's product portfolio in several privacy-conscious verticals. In the longer term the improved products and services should translate to overall increase of efficiency of business in these fields. Currently the primary advantages of the KSI blockchain over competing proposals are fast transaction finalization time (about one second on average) and low storage requirements of the main blockchain (about 2 GB per year). In order to maintain those properties, the computational efficiency of the added cryptographic primitives and protocols is of paramount importance.

4.1.3 Measures taken so far

Since the start of the PRIViLEDGE project, Guardtime's efforts in the healthcare sector have been organized into the dedicated Guardtime Health unit with an experienced team (www.guardtime.com/health) with several active projects ongoing in the field, including the Estonian Health Insurance Fund, the Health & Welfare Information Systems Centre, the North-Estonian Medical Centre, and the Tartu University Clinic, as well as the Division of E-services and Innovation of the Ministry of Social Affairs of Estonia.

4.1.4 Future plans

In particular, we are working with two potential clients specifically targeting the commercial deployment of outcomes of the cryptographic research from the PRIViLEDGE validated in the health insurance use case demonstration.

4.2 IBM Research – Zurich

4.2.1 IBM PRIViLEDGE goals

IBM participates in PRIViLEDGE to perform research and development tasks with the goal of advancing distributed ledger technologies, focused on, but not restricted to, the open-source platform Fabric. The two topics that IBM targets within PRIViLEDGE are flexible consensus and privacy of transactions. The importance of flexible consensus stems from the necessity of adapting DLT platforms to different use cases; the consensus mechanism represents one of the main trust assumptions of the platform, and a general-purpose platform such as Fabric must be adaptable to different scenarios, while delivering great performance in each of them. Transaction privacy is important for different reasons; one is that the confidentiality of business data requires to manage the visibility of data on a need-to-know basis, different from today's prevalent platforms that either store the data in clear (e.g., Bitcoin, Ethereum) or shield the data from everyone (e.g., ZCash). Another one is that service providers that leverage DLTs still have to comply with regulations such as GDPR, and proper cryptographic

mechanisms will be needed to achieve this requirement. IBM's goal in PRIViLEDGE is to advance the Fabric open-source platform in order to support these requirements.

4.2.2 Commercialisation

IBM's main exploitation route of PRIViLEDGE results is via integration of new technologies into Fabric. As many of IBM's blockchain-related offerings build on Fabric, the outcomes of PRIViLEDGE are expected to be instrumental for this area of IBM's business. The IBM Blockchain Platform integrates new features from Fabric and offers them to clients hosting their nodes with IBM. Improved technology and features in Fabric also help IBM in developing DLT networks that fulfill the needs of trade ecosystems as well as individual clients.

4.2.3 Measures taken so far

The measures taken so far can largely be subsumed under the topic of raising awareness. We have consulted multiple clients and government entities on blockchain technology, and discussed the necessity as well as the current state of privacy-preserving cryptographic technologies. We have presented PRIViLEDGE research and the goals of the project at the IOHK summit in Miami, FL. We have advocated for the use of privacy-preserving cryptography in Hyperledger Fabric within the Hyperledger community, and through multiple channels within IBM.

4.2.4 Future plans

We will continue our efforts to raise awareness with clients and partners, government entities, the Hyperledger Fabric as well as the academic community. As discussed above, IBM's exploitation of the results obtained in PRIViLEDGE is via generating open source code extending the Hyperledger Fabric platform. Fabric is then used by IBM in various client engagement as well as multiple services offered by IBM. Given this exploitation path, we will furthermore contribute code developed within PRIViLEDGE to the Hyperledger Fabric project.

4.3 University of Edinburgh

4.3.1 UEDIN PRIViLEDGE goals

The project team has incorporated material and research results of the project in courses related to the topic of the project. Among these are, most importantly, the Blockchains and Distributed Ledgers course (INFR11144), the Computer Security course (INFR10067) and the Introduction to Modern Cryptography course (INFR11131). UEDIN is collaborating with the industrial partner IOHK with which UEDIN has a long standing collaboration via its Blockchain Technology Laboratory. One of the aspects of this collaboration concerns the research for the Use Case 4. A partial outcome of this collaboration will be presented in the deliverable D4.1. UEDIN has also been involved in the designing aspects for the Diploma Use Case with the industrial partner GRNET. The project is also providing valuable professional training for the researchers involved and is enabling them to substantially broaden their command of distributed ledger technologies. The University of Edinburgh expects, as an outcome of this training, several publications in the top cryptographic and security venues such as CRYPTO, Eurocrypt, Asiacrypt, Public-Key Cryptography, Financial Cryptography, CT-RSA, IEEE S&P, and ACM CCS. Indeed, there are already research outputs, some of them in the form of accepted papers (to venues like ACM CSS and IEEE S&P) and some other under the form of preprint that will be submitted soon.

4.3.2 Commercialisation

UEDIN is a non-profit organization that will not perform commercial exploitation of the project results

4.3.3 Measures taken so far

Currently there are open problems that UEDIN is trying to solve with the mentioned partners within the scope of PRIViLEDGE. To keep track of the progress and make progresses that are consistent with WP1, WP3, WP4 and WP4, UEDIN has been involved in weekly meetings with the industrial partners and with the research partner UNISA.

4.3.4 Future plans

The future plan is to refine the research done so far for WP2, WP3 and WP4 and provide more research outputs related to the Use Cases and the Toolkits with particular attention to UC4 and UC3. Moreover, the results will be combined with software for e-voting which was developed by the team with previous funding from H2020 project PANORAMIX and the project DEMOS of the Greek secretariat of research and technology. The system is called Demos, and the combination with PRIViLEDGE will greatly enhance the system's verifiability as the system's security relies on a public bulletin board. Our objective is to roll out this system as a blockchain based service for UEDIN students during the course.

4.4 Technical University of Eindhoven

4.4.1 TUE PRIViLEDGE goals

The goals for the Technical University of Eindhoven in PRIViLEDGE are to extend its scientific knowledge in the DLT domain, building on the existing cryptography expertise. In particular, the goal is to study the use of secure multiparty computation in the context of DLT. Advanced research results will be submitted to toptier conferences and workshops in cryptography (mostly organized by IACR, ACM, and IEEE). Basic research results may also be integrated in advanced crypto courses taught at the TUE graduate school (master level) to keep these courses up-to-date with modern technology (e.g., in the course Applied Cryptography).

4.4.2 Results

Overall, the Technical University of Eindhoven seeks results in PRIViLEDGE that enhance its portfolio in privacy-protecting cryptographic protocols. Applications of secure multiparty computation with stronger security properties due to the use of DLT (e.g., by committing the inputs and outputs for secure computations using DLT) are of prime interest. Extending the MPyC framework with such DLT links is an example of a concrete result.

The Technical University of Eindhoven wants to strengthen its position as a knowledge partner in DLT, also at the national level within the Netherlands.

TUE's participation in PRIViLEDGE has identified concrete opportunities to apply its research on "Verifiable MPC" to the Blockchain setting. E.g. "private smart contracts" is an active area of development in the blockchain space that benefits greatly from the "public verifiability" achieved with "Verifiable MPC".

4.4.3 Measures taken so far

Conducted first research in how to apply the results of Trinocchio ("Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation", 2015) and Geppetri ("Pinocchio-Based Adaptive zk-SNARKs and Secure/Correct Adaptive Function Evaluation", 2017) in the blockchain context. TUE plans to present its findings on Verifiable MPC in the blockchain context during the PENCIL workshop prior to EUROCRYPT 2019 (May 18).

4.4.4 Future plans

Participation in PRIViLEDGE identified several highly valuable areas for (future) research and collaboration so far:

- TUE's work on Verifiable MPC can support relevant blockchain problem domains, such as private outsourcing and private smart contracts. This focuses on efficient on-chain verification of private & expensive off-chain work, involving multiple parties.
- TUE's work on Verifiable MPC (using SNARKs) could integrate well with UT's work on UC-secure CRS generation for SNARKs, and UT's work on more efficient privacy preserving smart contracts.
- TUE's extension of its MPyC library could prove valuable for GT's medical insurance use-case. Fit and requirements are actively explored between TUE and GT at the moment.

TUE's concrete next step is to enable "Verifiable MPC" and interaction with blockchain in its MPyC library. Second, we plan to achieve Verifiable MPC in other Zero-Knowledge Proof setups, most likely Bulletproofs.

4.5 University of Salerno

4.5.1 UNISA PRIViLEDGE goals

University of Salerno aims at producing important research results on privacy-enhancing DLT. More specifically, the research done at University of Salerno aims at improving the most useful privacy-enhancing cryptographic primitives (e.g., zero-knowledge proofs) and in strengthening the security and privacy of consensus protocols and smart contracts. Moreover University of Salerno expects high visibility for the produced results through invited talks and participations and organizations of panels, workshops and conferences. Last but not least, University of Salerno aims at starting joint projects with public or private organizations focusing on privacy-enhancing DLT. University of Salerno expects several publications from its members on advances in privacy-enhancing DLT. The main goal is to publish papers in top cryptography and security related venues such as CRYPTO, Eurocrypt, Asiacrypt, Public-Key Cryptography, Financial Cryptography, CT-RSA, IEEE S&P, and ACM CCS. Moreover University of Salerno expects solid partnerships with industry and public institutions that can leverage the research results achieved in PRIViLEDGE.

4.5.2 UNISA PRIViLEDGE results

University of Salerno will publish scientific results of both theoretical and practical relevance. Moreover University of Salerno will contribute to the organization of courses and seminars on privacy-enhancing DLT that will disseminate the achievements of PRIViLEDGE and will amplify its impact. Last but not least, University of Salerno will expand its network of collaborations with universities and industries both nationally and internationally.

4.5.3 Measures taken so far

none

4.5.4 Future plans

University of Salerno is currently focusing on security and privacy issues of consensus protocols and therefore expects to obtain new results in these topics.

4.6 University of Tartu

4.6.1 UT PRIViLEDGE goals

University of Tartu aims to use its research expertise in privacy-preserving technologies such as zero-knowledge proofs in various applications and use cases of the project. More precisely, for long time UT has been doing active research on various cryptographic protocols for e-voting and efficient zk-SNARKs that are two prominent tools for various use cases of the project. Particulry UT will focus on research on privacy-preserving cryptography (leading some of the tasks in WP2), background research on the design of cryptographic protocols needed for WP3 and collaboration with SCCEIV.

4.6.2 Commercialisation

University of Tartu is a non-profit organization that will not perform commercial exploitation of the project results.

4.6.3 Measures taken so far

none

4.6.4 Future plans

As University of Tartu is leaving the project, our main goal for the remainder of our stay in the project is delivering the contributions we promised up to the day of leave. However, we expect that the already involved people from UT will collaborate in the case of need for more discussion on achieved results by the day of leave.

4.7 Smartmatic-Cybernetica Centre of Excellence for Internet Voting

4.7.1 SCCEIV PRIViLEDGE goals

SCCEIV as an industrial partner in PRIViLEDGE provides use-cases to the partners for constructing DLTs and implements a working prototype of an online voting platform using improved DLTs.

SCCEIV expects distributed ledger technologies to provide additional transparency to online voting as a critical service. This means, that the voters and verifiers should be able to check that the software is working as expected. SCCEIV expects to improve privacy guarantees of the DLT based online voting platform to facilitate the public nature of the election audits.

4.7.2 Commercialisation

The expected outcomes of PRIViLEDGE will lead to improved offer for online voting on the organizational level providing third-party auditable online voting while protecting the privacy of the vote in long-term. DLT based auditing for online voting shall be part of SCCEIV offerings allowing SCCEIV to take part in procurements and increase interest with current and future customers. Finally, being a member of PRIViLEDGE reinforces SCCEIV's image as a novel and transparent online election services provider.

4.7.3 Measures taken so far

SCCEIV is currently redesigning workflows in it's product line to support homomorphic tally aggregation in DLT based scenarios.

4.7.4 Future plans

Upon finishing the prototype implementation SCCEIV intends to introduce it to its current customers and replace existing mixnet based installations with DLT based installations. SCCEIV has already described the approach to a few partners and the feedback has been positive. The new approach is seen to be more performance-efficient and allows integration with new key management platforms.

4.8 GRNET

4.8.1 GRNET PRIViLEDGE goals

GRNET aims at building the Diploma Use Case based on the results of PRIViLEDGE. On the deployment and service delivery side, this requires collaboration with industrial partner GUNET. On the development side, this requires collaboration with the research partners.

GRNET has already started developing a protocol that can be used for privacy-preserving certification of diplomas using DLTs. A basic requirement is that all steps of the certification process are captured on the ledger, so that they can be audited, and there can be no dispute that all steps necessary for a certification took place. Another essential requirement is that as little as possible of the certification information can be revealed to parties not involved in the certification per se. In particular, to certify a degree the only parties to which any information should be exchanged is the awarding institution, the graduate, and the entity to which the graduate wishes to provide evidence of the degree. Ideally, we would not like that entity to be able to pass on that information to any other party; moreover, nobody not involved in the certification process should be able to infer that a graduate submits a certification to a recipient.

In addition, GRNET works on developing a toolkit for the privacy-preserving data storage on ledgers. As DLTs may not be ideal vehicles for storing data, most current options opt for storing data off-ledger, while providing corresponding links on the ledger itself. GRNET is examining potential solutions.

Finally, there has been much interest in digital certifications by the European Commission. The European Blockchain Services Infrastructure (EBSI), developed under the auspices of the commission, has selected digital certifications for Diplomas as one of four use cases to be pursued by member countries. GRNET aims at building the Diplomas Use Case so that it is not incompatible with the proposals that will emerge from EBSI.

4.8.2 Commercialisation

The Diploma Use Case is not built for commercial profit, so there have been no activities for commercial exploitations of PRIViLEDGE's results by GRNET.

4.8.3 Measures taken so far

The protocol developed by GRNET is being analysed by PRIViLEDGE partners University of Edinburgh and University of Salerno. The target is to provide an analysis of the security requirements of the protocol and the underlying assumptions, so that implementation can then proceed.

GRNET has been following closely the developments of the EBSI, participating in the relevant meetings, and paying attention to the technologies proposed therein so that the PRIViLEDGE Diplomas Use Case. In parallel, GRNET is examining the technologies on Self-Sovereign Identity (SSI), which have been proposed as a potential solution to the problem of delivering privacy-preserving attestations of information to designated recipients.

In what regards the toolking for privacy-preserving storage on ledgers, GRNET has been studying approaches and technologies that are proposed for this particular problem. There is much activity on the topic lately, so GRNET is keeping track of different proposals with the aim of identifying designs that are compatible with th Diplomas Use case and that seem to have acquired momentum that augurs well for their long-term prospects.

4.8.4 Future plans

GRNET will intensify its efforts in the continuation of the project so that a viable product for the Diplomas Use Case will be delivered, as well as a toolkit for privacy-preserving data storage on ledgers.

4.9 GUNET

4.9.1 GUNET PRIViLEDGE goals

GUnet's main goal from PRIViLEDGE remains the assessment of DLTs and their comparative advantages in the implementation of decentralized solutions for the Higher Education. Specifically, in the endeavor to achieve an inter-university eDiplomas solution GUnet is exploring innovative yet practical solutions that will facilitate the processing of information located at distributed Students Information Systems (SIS) in a privacy preserving way. GUnet's primary goal is to evaluate these solutions in real world scenarios not only in terms of security but also in terms of functionality and performance.

Furthermore, GUnet in the framework of the PRIViLEDGE project has been intensively working with the Greek Universities for the standardization of the data structures and the semantics of the information which is required for the implementation of an eDiplomas solution.

4.9.2 Commercialisation

GUnet as a non-profit company has no commercialization plan in the strict sense. However, GUnet has a long history of offering complete software products—with no price-point attached to them—which are being widely use in production environments by educational organizations and other 3rd parties.

4.9.3 Measures taken so far

In the view of the upcoming diplomas UC implementation, GUnet has already implemented the basic APIs for the retrieval of the required informations from the Students Information System. The two biggest Greek universities have been actively engaged in this initiative and a dataset of more than 250K university diplomas has been used to construct synthetic yet realistic data for the PRIViLEDGE project.

4.9.4 Future plans

GUnet's future plans include the evaluation of DLTs to address auditing and accounting requirements at various stages of solution. Currently GUnet is evaluating along with the Greek Universities the idea to split in the digital world the public part of a diploma from the rest of the information that correlates it with a holder ie the holder's name, the issuing date, the grades etc. A public permissioned blockchain model could be used, for the announcement of the templatized part of the diplomas issued by each university which is anticipated to simplify the handling of the PII.

4.10 I.O.Research

4.10.1 I.O.Research PRIViLEDGE goals

I.O.Research expects the PRIViLEDGE project to contribute, in accordance with the project's goals, to a better general understanding of the methods for maintaining privacy on a decentralized ledger, as well as methods for secure decentralised updating of the ledger protocol and the blockchain system in general. The hope of I.O.Research is that these methods will be (directly or indirectly) applicable to the Cardano blockchain maintained by IOHK, as well as other DLT projects that IOHK is involved in.

Both of these problems are highly relevant in the context of permissionless blockchain systems. While there exist several deployed permissionless blockchains providing some privacy guarantees to its users, none of

these uses proof of stake as its underlying consensus mechanism. The reason is that the combination of privacy-preserving constructions and stake-based consensus (where the stake is recorded on the privacy-preserving ledger itself) introduces additional technical challenges. I.O.Research hopes to benefit from the research performed in the course of the PRIViLEDGE project when addressing these challenges for Cardano.

In addition, decentralising software updates is a difficult problem, mainly because it entails a secure governance process, where decisions on the roadmap of the system will be taken collectively and not centrally. Moreover, today even in permisionless public blockchain systems software updating is assumed by a central authority (the main maintainer), who takes decisions on the roadmap of the source code and also provides guarantees for the security of the updated software. All in all, the decentralization of software updates radically changes the way public blockchain systems are maintained today, as it removes all central authorities from all the decision points in the lifecycle of a software update.

The Cardano blockchain system is built based on a roadmap, whose basic pillars are: decentralization, interoperability, privacy, expressibility & programmability, sustainability & governance, scalability, high throughput & low latency and effective incentive structure. All these constitute fundamental goals to be incorporated into our blockchain technology. The privacy preserving ledger problem directly impacts the privacy pillar, while the decentralised software updates problem is directly related to the sustainability & governance pillar. Therefore, there is a direct connection between the results of the PRIViLEDGE project and the fundamental goals in the roadmap of the Cardano blockchain product. Thus, our ultimate goal is to leverage the PRIViLEDGE results towards fulfilling these goals by influencing significantly the future releases of the product.

4.10.2 Commercialisation

I.O.Research expects that given the above-described research outcomes, their implementation in the Cardano blockchain by IOHK may provide a competitive advantage to the project, increasing its commercial success. This expectation is based on the current understanding that both privacy-supporting features, as well as a secure update mechanism, are seen as important (and often missing) aspects of existing projects in the cryptocurrency space.

Moreover, privacy as well as sustainability and governance are some of the basic pillars in the vision of the Cardano product and have been set as clear goals for its future releases. Therefore, there is a direct connection between the PRIViLEDGE project results and the goals in the roadmap of the Cardano product. We strongly believe that privacy enabled transactions on the one hand, is a key feature for opening up the blockchain technology to other areas beyond cryptocurrencies and decentralised software updates on the other hand, are a key component in the governance process of a permissionless blockchain system. Therefore we aim at leveraging significant results from the PRIViLEDGE project by strengthening our product proposition by offering better privacy preservation features and an open community-based governance and software maintenance process.

4.10.3 Measures taken so far

In order to realize our goal of exploiting PRIViLEDGE project's results for influencing future releases of the Cardano blockchain product, several measures have been taken. An internal IOHK and IORESEARCH team has been set up for discussing all the relevant issues that emerge from the PRIViLEDGE project results. It is essential that in this dedicated team there are representatives from all the core teams that drive the evolution of the Cardano product, namely: the Engineering team, the Research team and the Product Management team. Moreover, a dedicated Slack channel has been created for the collaboration of this internal team and for discussing anything that is related to the results coming from the PRIViLEDGE project.

In addition, a very close collaboration scheme has been set up with UEDIN, in order to closely work on the problems of decentralised updates and privacy. In particular, a periodic working meeting has been established, where IOResearch and UEDIN researchers meet and discuss core work topics and evaluate progress on a weekly basis. Moreover, periodic meetings with the Chief Scientist of IOHK are conducted on a regular basis and work status is reported and direction is given on difficult issues that arise.

Finally, in order to better identify opportunities for incorporating PRIViLEDGE project results into the Cardano blockchain system, an in-depth as-is analysis of the current software update mechanism has been performed. Furthermore, a gap analysis with respect to the posed requirements (deliverable D1.1) has been conducted. A significant part of this analysis will be included in the deliverable D4.1.

4.10.4 Future plans

For our next steps, we plan to analyse the design and functional specification of the update mechanism for the upcoming Cardano release (code named "Shelley"). With this release, Cardano essentially will open up to public. It is the release, where the product will move from a federated setting, where only a specific set of keys could participate in running the protocol, to a decentralized setting, where potentially any stakeholder can participate. This release has some interesting features that are in direct correspondence with the update mechanism that we work on the PRIViLEDGE project. One such feature is the delegation to stake pools for managing the stake and participating in the protocol, in the stakeholder's stead.

Furthermore, we plan to engage even more the IOHK engineers in the design process of the prototype that will be developed in the context of the 4th use case of the PRIViLEDGE project. This will ensure that our prototype will be in conformance with the design practices followed by IOHK and secure the possibilities to influence the actual Cardano implementation. Finally, we plan to engage the Cardano project management team, in order to identify further synergies and discuss potential Cardano releases that PRIViLEDGE project results could be incorporated.

5 Conclusion

PRIViLEDGE set off with a strong publication output starting in July 2018. Overall, 11 papers have been published to date, with 5 of them at top-level conferences explicitly targeted by PRIViLEDGE according to the project proposal. Another 14 papers are currently at different stages of the publication cycle, some of them already publicly available on preprint servers, others in submission to conferences. This indicates that the publication output will remain strong in the coming months.

Project partners have given 17 presentations on PRIViLEDGE research outcomes at various venues, focused mostly on an academic audience as appropriate for the current phase of the project. Venues ranged from small, specialized workshops with ~ 40 participants all the way to large, general conferences with several hundreds of people in the audience. The early publications that have been put online between July and October 2018 have garnered their first citations; although it is still very early for drawing conclusions, it is also clear that some works have already seem encouraging uptake by the research community.

The PENCIL workshop organised by PRIViLEDGE as an affiliated event of Eurocrypt 2019 made the project widely known in the academic community. With 120 participants, PENCIL was the largest workshop at this year's Eurocrypt conference. The positive feedback after the workshop showed that the community appreciated the concept of the workshop, and indicated that PRIViLEDGE gained visibility in the academic community.

A very important type of impact for PRIViLEDGE research results is through their use in the toolkits and prototypes created by the project. To make sure that research results can actually be taken up by use-case partners, we created teams within the project that explicitly connect use-case partners with academic partners for the benefit of both. Following this, partners have updated and extended their exploitation plans from Deliverable 5.3, which set out a path for the exploitation of the results and toward achieving practical impact.