DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D5.4 – Updated Consolidated Communication and Dissemination Plan

Due date of deliverable: 31 December 2018
Actual submission date: 21 December 2018

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

Lead contractor: Guardtime AS
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	

D5.4

Updated Consolidated Communication and Dissemination Plan

Editors
Tuuli Lõhmus (GT)
Mirjam Kert (GT)

Contributors
all partners

Reviewers
Björn Tackmann (IBM)
Toomas Krips (UT)
Karim Baghery (UT)

21 December 2018
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.

Executive Summary

In addition to the core activities, the success of the project depends largely on the quality of dissemination and exploitation activities. PRIViLEDGE therefore contains a separate work package, WP5, that coordinates the impact-creating activities of the project, including dissemination and exploitation activities.

The current document describes the updated communication and dissemination strategy of PRIViLEDGE and is central to all activities that will be implemented towards relevant stakeholders and interested parties. This document gives an overview of the communication and dissemination activities undertaken during the first 12 months of the project as well as plans for the upcoming months.

Contents

1 Introduction

D5.1 Initial Communication and Dissemination Plan identified and classified the target audience, the dissemination methods and goals, and the measures to assess the impact of the dissemination activities to ensure proper dissemination of the generated knowledge with regards to confidentiality, publication, and use of the knowledge.

The current document describes the updated communication and dissemination strategy of PRIViLEDGE and is central to all activities that will be implemented towards relevant stakeholders and interested parties. The document outlines specific activities undertaken during the first 12 months of the project as well as plans for the upcoming months and any changes in the original plan.

2 General Strategy for Dissemination and Communication

2.1 Purpose

The overall aim of the dissemination activities is to ensure a positive impact through engagement with the stakeholders in the fields that benefit most from the results of the project. For this purpose, the updated dissemination and communication plan will outline reviewed and updated channels and methods to ensure that the project research and practical outcomes are widely disseminated to the appropriate target audiences at appropriate times along the project lifecycle. The updates and changes in the plans and strategies are based on the experiences of communication activities during the first year.

The objectives of the communication and dissemination activities are:

- Raising awareness of the problems the project is aiming to solve,
- Creation of awareness about the project among the target audience,
- Promotion of the innovations of PRIViLEDGE within the research and industry communities, and
- Ensuring that any additional application to the potential exploitation is taken into account.

The first item has been added to the list compared to the previous communication and dissemination plan to ensure both general and target audience is aware of the challenges faced by different sectors. A clear communication of the present problems will help to promote innovations of PRIViLEDGE as relevant communities can be aware of the problems and solutions. As originally planned, dissemination activities will continue in raising awareness of the project results and gathering the necessary feedback as well as building understanding and facilitating adoption of the results by the different stakeholder groups who can directly benefit from the project. Communication activities will complement the PRIViLEDGE dissemination activities towards increasing the outreach of the project's results and enhancing its visibility to stakeholders out of the core target groups who can directly benefit from the project, permitting a two-way exchange.

2.2 General Strategy

All consortium partners are contributors to the dissemination and communication activities under WP5: Communication, Dissemination, and Exploitation lead by Guardtime. The communication and dissemination activities are managed via the communication channel on Slack as well as the mailing list. All communication materials are uploaded and maintained on GitHub.

Main communication and dissemination channels throughout the project are planned to be:

1. Offline channels
    - Business relationships
    - Conferences

- Scientific publications
- Workshops and seminars
- Industry meetings
- Policy meetings

2. Online channels

- Website - main point for people finding out about the project and wanting to know more
- Social Media
- Press releases and blogposts at partners' websites

Key Messages. The message component of the dissemination and communication strategy comprises of the set of arguments, reasons and facts to be used to inform the targeted audiences of the value in using PRIViLEDGE results. Key messages are intended to deliver relevant and meaningful content suited to communicate the PRIViLEDGE value proposition. The PRIViLEDGE project has the high level key message and a number of supporting key messages.

High level message: *"The PRIViLEDGE project aims to develop cryptographic protocols enabling privacy, anonymity, and efficient decentralised consensus for distributed ledgers and blockchains"*.

Supporting messages:

- PRIViLEDGE improves cryptographic schemes protecting security and privacy in applications such as encrypted data on the Internet and online payments, leveraging tools such as privacy-preserving mechanisms and post-quantum cryptography, while focusing on the emerging distributed ledger technology;
- PRIViLEDGE shows how to perform practical, secure and privacy-preserving transactions by making use of distributed ledgers;
- PRIViLEDGE features four heterogeneous real-world use cases to show concrete examples of the validity of the developed technology;
- PRIViLEDGE bridges the gap between theory and practice for the deployment of a cybersecurity infrastructure based on distributed ledgers;
- PRIViLEDGE addresses the tension between the transparency provided by the emerging distributed ledger technologies and the strict requirements for data privacy.

All of the key messages have remained unchanged during the first year. The supporting messages will be expanded with more information and examples as the project develops.

Target Audience. The dissemination and communication activities aim to ensure impact creation by engaging with the stakeholders that can gain most from the project results and will leverage the consortium members' strong relationships with a range of audiences: industrial, academic/research, and governmental. The primary target audience will be the relevant industry sectors, which include those directly related to the PRIViLEDGE use cases and security and privacy providers.

- **Industry**: e-voting, insurance, higher education, systems management, other applicable sectors
  Main channels: Existing business relationships, policy reports, meetings, conferences, seminars/ workshops, meet-ups
  Reasons: To engage the industry in the research; to inform them of the issues addressed by the consortium and to invite them to comment on the recommendations made by the consortium.

- **Security and privacy providers**
  Main channels: Existing business relationships, policy reports, meetings, conferences, seminars/ workshops, meet-ups
  Reasons: To engage them in the up-take of innovation that PRIViLEDGE produces.

- **Research and scientific community**
  Main channels: Academic publications, journals, conferences, workshops
  Reasons: To engage them in dialogue, to present them research results and ignite further academic work.

- **Public sector**
  Main channels: Policy reports, meetings, conferences, workshops, social media
  Reasons: To engage them in the relevant research for their purposes such as the e-voting use case that PRIViLEDGE will develop.

- **General public**
  Main channels: Policy reports, meetings, conferences, workshops, social media
  Reasons: To engage the public in a debate on security and privacy.

The target audience remains the same as identified at the start of the project.

Visual identity. A visual identity of PRIViLEDGE was created at the beginning of the project. The PRIViLEDGE logo expresses security and privacy by having the letter "I" shaped like a padlock. This visual identity is used in all the dissemination outputs, such as the project website, social media accounts, the project videos and leaflets, etc.

Figure 1: Project logo.

Open Access. PRIViLEDGE will continue to pursue an open-access policy, making results and publications publicly and freely available with a green or gold open-access policy.

"Green" open-access publication or "self-archiving" is today in line with the policy of major institutions and associations (e.g., ACM, IEEE, Springer) of the most selective and recognised conferences and journals. Within this policy, the publishers allow authors to post the final versions of the accepted papers in their personal web site, the web site of their employers, or selected pre-authorised institutional web sites. Project publications will therefore be posted on the appropriate web sites among these and linked from the web site of the project, thus ensuring broad visibility and easy access. This covers distribution even before a formal reviewed publication and allows early access to the work by the community. Examples of suitable open-access publication venues are the ACM Computing Research Repository (CoRR, arxiv.org) and the Cryptology ePrint Archive (`eprint.iacr.org`). Furthermore, the partners' institutional archives and other open archives will be used for providing dissemination.

In "gold" open access, the publisher version of the publication is openly accessible. This method often incurs a publication fee paid by the authors' institutes.

3 Overview of Activities during M1-M12

3.1 Online Communication

3.1.1 Website

The main PRIViLEDGE dissemination channel is and has been for the first year the official website (`www.priviledge-project.eu`), presenting the project and its on-going activities as well as all the public deliverables and published research. The updated website design ensures a high level of accessibility and usability. The menu gives direct access to six main pages: the "About" page with a general description of the project, objectives and work packages, technology introduction, project use cases, and introduction of the coordinator. The second section "Consortium" gives an overview of the partners involved and their roles in the project. The third section "Publications" consists of the project deliverables and publications which have been produced. The section "Events" gives an overview of past and upcoming events and provides links to respective pages. News and news archives are included under the "News" section. The final section "Contact" contains the Coordinator contact as well as the social media link.

Figure 2: Top half of the project homepage.

During the first 12 months of the project, there have been over 1800 visits of the homepage with approximately 1250 unique visitors. The page for the upcoming workshop PENCIL has had more than 800 visits in less than four months. As the workshop advertising is at the early stage, the visitor numbers are predicted to grow rapidly during M13-M17.

3.1.2 Twitter

The purpose of a Twitter account is to reach wide and targeted audiences in a fast and efficient manner. Social media is used to communicate main events as well as general news related to the project. It is also a tool for disseminating project results to specialist audiences.

For the above mentioned purpose, an account for the project has been created in Twitter `https://twitter.com/PRIViLEDGE_EU`. The project partners help to enhance the project outreach by retweeting. The PRIViLEDGE Twitter account is and will be used to inform the broader European cybersecurity and cryptography community and the wider public about the project's objectives and technical developments as they occur.

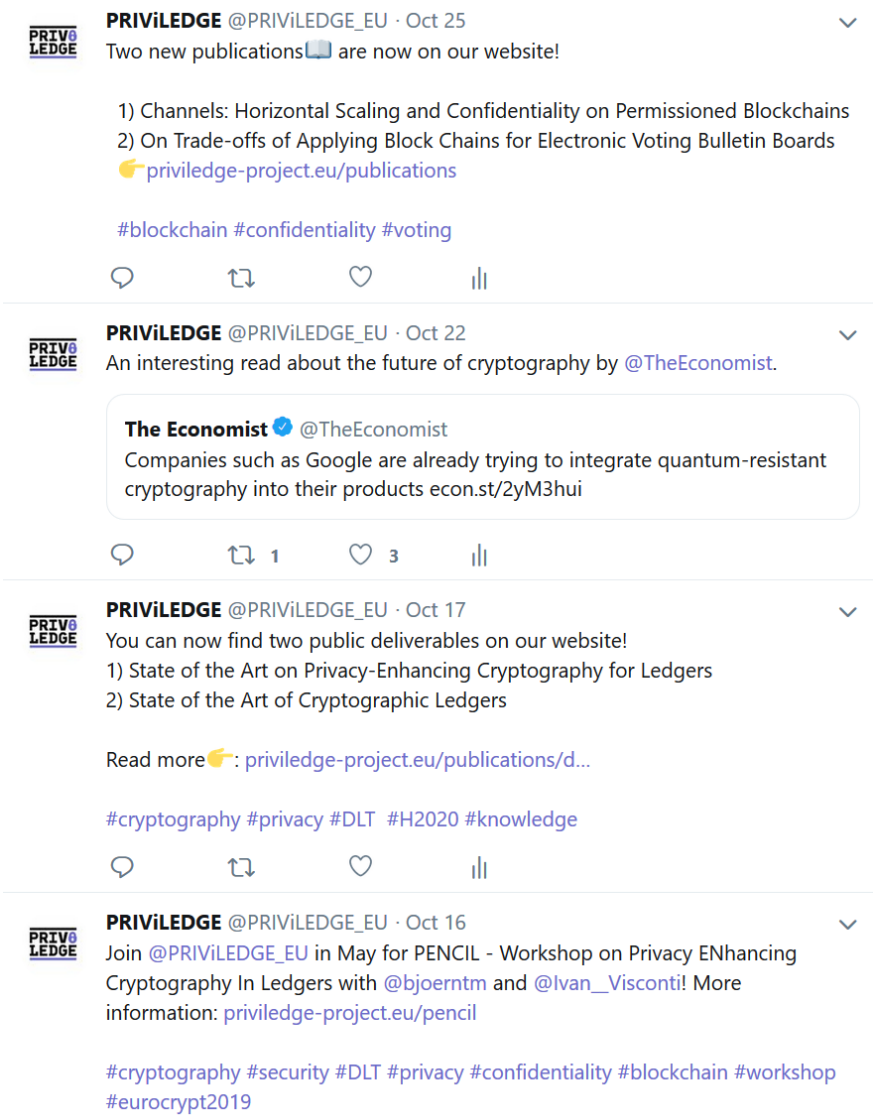

Figure 3: Twitter timeline example from October 2018.

Twitter is also used for starting and participating in wider discussions about privacy and the use of cryptography, both topics are extremely relevant across all industries and around the globe. This aligns with the general strategy for raising awareness of the issues as well as informing general public about the PRIViLEDGE methods. An example of Twitter timeline is shown in Figure 3.

Twitter plan. A specific Twitter plan has been developed by Guardtime and shared with the rest of the Consortium, to coordinate the activities of the partners and guarantee a coherent approach. The Twitter plan is in Appendix 4.3.

3.2 Offline Communication

3.2.1 Published Papers, Proceedings, and Reports

Formal academic publishing. PRIViLEDGE project has strong scientific foundation and some of the research results have already been published in conferences with formal proceedings.

1. Androulaki E., Cachin C., De Caro A., Kokoris-Kogias E. (2018) Channels: Horizontal Scaling and Confidentiality on Permissioned Blockchains. In Lopez J., Zhou J., Soriano M. (eds) Computer Security. ESORICS 2018. Lecture Notes in Computer Science, vol 11098. Springer, Cham

2. Heiberg, S., Kubjas, I., Siim, J., & Willemson, J. (2018). On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards. E-Vote-ID 2018, 259.

3. Kiayias, A., Kuldmaa, A., Lipmaa, H., Siim, J., & Zacharias, T. (2018). On the security properties of e-voting bulletin boards. In International Conference on Security and Cryptography for Networks (pp. 505-523). Springer, Cham.

4. Ciampi, M., & Orlandi, C. (2018). Combining private set-intersection with secure two-party computation. In Dario Catalano and Roberto De Prisco, editors, Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings, volume 11035 of Lecture Notes in Computer Science, pages 464–482. Springer, 2018.

5. Badertscher, C., Gazi, P., Kiayias, A., Russell, A., & and Zikas, V. (2018). Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pages 913–930, 2018.

Technical reports.

- Bouman, N. J., & de Vreede, N. New Protocols for Secure Linear Algebra: Pivoting-Free Elimination and Fast Block-Recursive Matrix Decomposition. Cryptology ePrint Archive, Report 2018/703. https://eprint.iacr.org/2018/703.

- Garay, J. and Kiayias, A. SoK: A consensus taxonomy in the blockchain era. Cryptology ePrint Archive, Report 2018/754, 2018. https://eprint.iacr.org/2018/754.

- Kiayias, A. and Zindros, D. Proof-of-work sidechains. Cryptology ePrint Archive, Report 2018/1048, 2018. https://eprint.iacr.org/2018/1048.

- Kiayias, A. and Russell, A. Ouroboros-BFT: A simple Byzantine fault tolerant consensus protocol. Cryptology ePrint Archive, Report 2018/1049, 2018. https://eprint.iacr.org/2018/1049.

3.2.2 Talks and Presentations at Events

PRIViLEDGE partners have given a number of talks and presentations about the project work. Those events have given an excellent opportunity for security providers and scientific community to learn more about the specific research as well as more about the project in general.

Conferences.

- Michele Ciampi (UEDIN): "Combining private set-intersection with secure two-party computation." Talk, Security and Cryptography for Networks 2018, Amalfi, Italy, Sept. 2018.

- Ivan Visconti (UNISA): "Blockchain Technology Beyond Cryptocurrencies." Keynote talk at session "Blockchain technologies: challenges and opportunities", 4th International Forum on Research and Technologies for Society and Industry (RTSI 2018), Palermo, Italy, Sept. 2018.
- Sven Heiberg (SCCEIV), Ivo Kubjas (SCCEIV), Janno Siim (UT) and Jan Willemson: "On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards." Third International Joint Conference on Electronic Voting, Bregenz, Austria, Oct. 2018.
- Christian Cachin (IBM): "Distributing trust with blockchains." Keynote talk, 17th International Conference on Cryptology And Network Security (CANS 2018), Naples, Italy, Oct. 2018.
- Ivan Visconti (UNISA): "Delayed-Input Cryptographic Protocols." Keynote talk, 17th International Conference on Cryptology And Network Security (CANS 2018), Naples, Italy, Oct. 2018.

Workshops.

- Berry Schoenmakers (TUE): "MPyC – Python Package for Secure Multiparty Computation." A talk in Theory and Practice of Multiparty Computation (TPMPC) 2018 Workshop in Aarhus, Denmark, May 2018.
- Christian Cachin (IBM): "Distributed trust – From Byzantine consensus to blockchain." Keynote talk, chain-in: International Industrial & Academic Conference on Blockchain Technology, Porto, Portugal, July 2018.
- Christian Cachin (IBM): "Hyperledger Fabric – A platform for distributing trust." Workshop on Decentralized Cryptocurrencies and Blockchains, Crypto 2018, Santa Barbara (CA), USA, August 2018.
- Christian Cachin (IBM): "Asymmetric Distributed Trust." Dagstuhl Seminar on Blockchain Security at Scale, Dagstuhl, Germany, November 2018.

Other events.

- Berry Schoenmakers (TUE): "Crypto Circus: Zeroknowledge and MPC Explained". A talk at Norwegian University of Science and Technology. Trondheim, Norway, February 2018.
- Ivan Visconti (UNISA): "Blockchain Technology: A Cryptographic Perspective." Invited talk, part of Cryptography Seminar Series at University of Oxford, UK, April 2018.
- Helger Lipmaa (UT): "ZK-SNARKs: foundations and applications." Number theory and coding theory: Contemporary applications in security Summer School. Turku, Finland, June 2018.
- Christian Cachin (IBM): "Secure distributed programming for blockchains." 14th LASER Summer School on Software Engineering, Tutorial. Elba, Italy, June 2018.
- Christian Cachin (IBM): "Distributing trust with blockchains." CERN Colloquium, Geneve, Switzerland, July 2018.
- Ivan Visconti (UNISA): Meeting "Initial Coin Offering (ICO)" to discuss the security of current blockchains and how thing will change with PRIViLEDGE, Consob, Milan, Italy, July 2018.
- Karim Baghery (UT): "The Bitcoin Lightning Network." Presentation at Iran Telecommunication Research Center (ITRC), Tehran, Iran, July 2018.
- Karim Baghery (UT): "Introduction to ZK proofs and SNARKs." Presentation at Sharif Blockchain Lab, Sharif University of Technology, Tehran, Iran, July 2018.

- Karim Baghery (UT): "A Subversion-Resistant SNARK." Presentation at Information Systems and Security Lab (ISSL), Sharif University of Technology, Tehran, Iran, Aug. 2018.
- Christian Cachin (IBM): "Distributed trust - From Byzantine consensus to blockchain." 1st ACM SIGOPS Summer School on Advanced Topics in Systems (SATIS '18), Tromsø, Norway, Aug. 2018.
- Helger Lipmaa (UT): "On QA-NIZK in the BPK model." Talk during Joint Estonian-Latvian Theory Days in Riga, Latvia, Oct. 2018.
- Janno Siim (UT): "On the Security Properties of e-Voting Bulletin Boards." Talk during Joint Estonian-Latvian Theory Days in Riga, Latvia, Oct. 2018.
- Helger Lipmaa (UT): "On QA-NIZK in the BPK model." Presentation at at Simula@UiB, Bergen, Norway, 2018.

3.2.3 Attended Events

All the attended events have given an excellent opportunity for project partners to interact directly with security providers and scientific community so the project and its aims and developments are well-known in the community.

Conferences.

- Björn Tackmann and Christian Cachin (IBM): Real World Crypto, January 10-12, Zurich, Switzerland
- Ivan Visconti (UNISA): ITASEC (Italian Conference on Cybersecurity), February 6-9, Milan, Italy
- Christian Cachin (IBM), Ivan Visconti (UNISA), Berry Schoenmakers (TUE): Eurocrypt, April 29-May 3, Tel Aviv, Israel
- Christian Cachin (IBM): Crypto, August 19-23, Santa Barbara, US
- Christian Cachin (IBM): Asiacrypt, December 2-6, Brisbane, Australia

Workshops.

- Niels de Vreede (TUE): Theory and Practice of Multi-Party Computation, May 28-31, Aarhus, Denmark
- Björn Tackmann (IBM): IoT Conference, September 12, Bern, Switzerland
- Ivan Visconti and Luisa Sinicalchi (UNISA): Theory of Blockchains and Cryptocurrency, October 6, Paris, France
- Luisa Sinicalchi (UNISA): Workshop on Blockchain Technology and Theory, July 23, London, UK.

Other events or meetings.

- UT: Participated in COST Training School on Symmetric Cryptography and Blockchain. Torremolinos, Spain, February 2018.
- GT: Participated in an event organised by North European Cyber Security Cluster (NECSC).
- TUE: Participated in Coalition Day by DBC Dutch Blockchain Coalition at ABNAMRO headquarters, Amsterdam, The Netherlands, June 2018.

- GT: Participated in an event organised by European Cyber Security Organisation (ECSO).
- UT: Participated in 14th LASER Summer School on Software Engineering, Software Technology for Blockchains, Bitcoin and Distributed Trust Systems. Elba, Italy, June 2018.
- GRNET and GT: Participated in meetings organised by European Blockchain Partnership.
- GT: Participated in a meeting with Estonian Information Security Association.
- UNISA: Symposium: Can The World Run on Blockchains? The Good, The Bad, and The Ugly. Darmstadt, Germany, September 2018.

3.3 Monitoring and Evaluation

The results of the communication and dissemination strategy are constantly monitored in order to assess its effectiveness and progresses, as well as to formulate change requirements where necessary. For each dissemination channel some Key Performance Indicators (KPIs) were identified at proposal stage. The originally identified KPIs are shown in Table 1 along the corresponding metrics for the first year. The comments reflect the reasons for any deviations as well as some plans for the future. An adjusted set of KPIs are proposed in Table 3 with further explanations for any changes detailed in Section 4.3

4 Plans for M13-M36

This section outlines more specific plans and actions for the next years to implement the strategy from Section 2.

Dissemination of project results as well as open access to scientific publications and research data is governed by the procedure described in Article 29 of the EC Grant Agreement (EC-GA).

4.1 Plans for M13-M36

PRIViLEDGE will continue to work on communication and dissemination to archive aims set out in Section 2.1 and keeping activities aligned with Exploitation Strategy and Roadmap. KPI metrics are adjusted based on the analysis of the first year in Section 3.3.

Organising workshops.

- Workshop 1 is PENCIL workshop detailed in Section 4.2. It will take place on M17.
- Workshop 2 is dedicated to deliver and demonstrate PRIViLEDGE use cases to specific target audiences; also in the second half of the project when the work is ready to be presented. This workshop is planned for the second half of year 2, between M18-M24. The details of the workshop are not finalised yet.
- Workshop 3 is dedicated to exploitation of PRIViLEDGE results; the objective is to perform expert interviews and focus groups. This is planned for third year of the project, after M25.
- Workshop 4 is dedicated to delivering policy recommendations to relevant stakeholders from industry, public sector and standardisation communities; this workshop is envisaged towards the end of the project, most likely during the last 6 months.

Exhibiting in conferences and workshops. The PRIViLEDGE project aims to exhibit its results in various conferences by having a special exhibition area, communicating via dedicated panels, and presentations. We are interested in participating in events like ICT 2019, The Annual Privacy Forum and other events organised by the European Commission.

KPI	Achieved M1-M12	Planned M1-M12	Comments
Events attended representing the project	15+	10	Excellent first year mostly due to active participation of research partners in conferences and various academic events.
Business events attended	5	3	A number of cybersecurity related events relevant to different use cases.
Communication with SMEs	8	10	Most communication with SMEs was related to e-voting, insurance and blockchain technologies.
Communication with other relevant industry	7	5	Both academic and industry partners were active in industry communication.
Communication with end users	9	10	A variety of events and direct meetings have taken place both by academic and industry partners.
Publications in peer-reviewed journals and conferences	5	1	Excellent scientific work on e-voting, blockchains, and secure computing has been published in journals and conference proceeding. More publications have been approved and will be published soon.
Press/general media articles published	0	5	This KPI will be not be used in the future (explanation in Section 4.3), but general media articles about PRIViLEDGE will be linked from the website.
Workshops of the project	0	0	PENCIL workshop is planned for M17.
Press releases	2	5	The project development has been at relatively early stages and no press releases have been made since announcing the start of the project. In the future, press releases could be used for workshops or other events but are not part of KPIs.
Website visitors	1700	3000	The numbers are increasing and most of the visits were made after M8.
Mentions of PRIViLEDGE in other websites	15+	10	For example news about the project, mentions on partners' websites and PENCIL workshop-related mentions on Eurocrypt 2019 website.
Downloads from PRIViLEDGE website	-	200	This metric has not been relevant as most content can be seen without downloading it. All deliverables and scientific publications are on the website and visitors have an easy access to them. Scientific publications have had several hundred downloads from the publisher's source.
Followers on social media (Twitter)	52	100	The number of followers is increasing and the plan is to promote the account on more events and workshops.

Table 1: KPIs for M1-M12.

Scientific contribution. The PRIViLEDGE project research results will be published in the main peer-reviewed journals and conferences with formal proceedings. Several research papers are in preparation and are expected to be submitted for publication in early 2019. In addition to conferences with formal proceedings, also informal workshops and seminars, such as the Real-World Cryptography Conference and various regional and local workshops and summer schools, will be used to present the research results of PRIViLEDGE.

Educational contribution. The project teams in academic partners will incorporate material and research results of the project in courses related to the topic of the project, for example courses on blockchains and distributed ledgers, and on cryptography. Also, project partners will give talks, seminars and short lecture courses on their research.

Visibility and informing both possible future partners and general public. Following activities and communication materials/methods are planned and/or updated to better communicate the project work:

1. A project blog with monthly updates. The blog will be a way to gain further insight into the project theory and development of different use cases. Each partner will contribute at least one post per year. The tentative planned schedule is in Table 2.

2. A video to introduce PRIViLEDGE aims and methods. The scenario will be developed during M13-M18 with all the partners. Later, this video can be widely used to promote the project and direct audiences to the project website to study further details.

3. Regular news on homepage about project use-cases, events and plans. The news section will be regularly updated at least once per month to ensure latest information and events are shared promptly and widely.

4. A visual update for the webpage. The project website will be updated to create more intuitive and balanced user experience. The proportions of the pages will be adjusted and more linked sections added to ensure first time visitor find a way around and returning visitor can easily find the latest news, blog entries, event information and reading materials. The design and colour palette will be reviewed and slightly expanded. The update will take place during M13-M18.

5. An event calendar with information where project partners can be seen and heard. To avoid getting information after the occasions, all partners can contribute to calender visible on the website before attending conferences, workshops or open seminars. The main benefit of this is the opportunity for interested audiences to engage directly with project partners.

6. Updated leaflets and visual materials for workshops/conferences. The main update will be based on the final use-cases defined by the end of first year. The updated materials will be ready before the first workshop on M17.

Engaging with industry partners and end-users. PRIViLEDGE consortium members also have strong presence in industry circles. Exploitable results of the project will be presented at applicable business sector conferences and general distributed ledger technology events such as CONSENSUS and Blockchain Week. Also, partners will participate in various events organised by North European Cyber Security Cluster (NECSC), European Cyber Security Organisation (ECSO), and European Blockchain Partnership (EBP).

Policy presentations. Project results will be disseminated at the relevant European fora such as the cybersecurity public-private partnership hosted by the ECSO as well as other relevant public private partnerships and industry forums.

The European Blockchain Partnership was tasked to identify a set of cross-border use cases that should be implemented in the European context and would benefit from a European Blockchain Services Infrastructure

Table 2: Blog post plan for 2019 with responsible partner

Time	Responsible partner	Preliminary topic (if already known, otherwise will be determined later)
January 2019	GT	Project year overview for 2018. Introduction to blog format.
February 2019	UT	-
March 2019	UEDIN	-
April 2019	IBM	-
May 2019	GT?	PENCIL Workshop
June 2019	GUNET	-
July 2019	SCCEIV	-
August 2019	GT	-
September 2019	UNISA	-
October 2019	TUE	-
November 2019	GRNET	-
December 2019	GT	Project year overview - technical progress and events during 2019.

(EBSI). Greece, through the GRNET representative, along with a number of other countries, argued for a use case implementing digital certificates, which will stronly complement the diplomas use case of PRIViLEDGE. After deliberations, the "Certification of Diplomas / Qualifications" was selected as one of five use cases, whose implementation will be actively promoted with member states committing to their realisation (the other four use cases relate to the exchange of excise data, the distributed registry of an Import One-Stop-Shop VAT registration number, a registry of audit-related files for the European Court of Auditors, and Self-Sovereign Identity for Public Services linked to eIDAS).

The inclusion of the "Certification of Diplomas / Qualifications" is a big boost for the PRIViLEDGE diplomas use case, and will be actively pursued for all possible synergies in the coming years.

4.2 Preparation for Upcoming Events

The project includes preparing and delivering four workshops. The first of these will take place in May 2019 in Darmstadt, Germany at the same time and place as Eurocrypt, one of the top international conferences in the cryptography.

PENCIL - Workshop on Privacy ENhancing Cryptography In Ledgers on May 18, 2019, Darmstadt, Germany. The purpose of the workshop[1] is to bring together researchers and practitioners working in cryptography, security, and distributed systems from academia and industry, who are interested in cryptographic techniques for improving the privacy of blockchains and their protocols. The main goal is to foster information exchange between attendees from the different areas, to present new developments in cryptographic schemes and protocols, as well as applications and challenges in order to stimulate both use of new cryptographic techniques to improve DLT-based systems as well as future cryptographic research targeting applications in DLT.

The workshop on Privacy-Enhancing Cryptography in Ledgers aims at discussing questions of confidentiality, privacy, scalability, and integrity in the context of distributed ledger technologies and cryptocurrencies. The workshop solicits submissions describing current work addressing decentralized cryptocurrencies and distributed ledger technologies, including cryptographic schemes and techniques, analytical results, work on systems, and/or position papers, with a focus on the area of privacy and confidentiality.

PENCIL workshop is an affiliated event of Eurocrypt 2019[2] which takes place on May 19-23 in Darmstadt,

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

Germany. Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR). The same location and affiliation of the workshop with the conference provides an excellent participation opportunity for world leading researchers and practitioners.

The main organisers are Björn Tackmann (IBM) and Ivan Visconti (UNISA).

4.3 Monitoring and Evaluation

The KPIs are slightly adjusted to better reflect the academic contribution through scientific collaboration. Some modifications for KPIs are planned:

- Categories of 'business events' and 3 separate communications 'with SME/other relevant industry/end-users' are merged into one to avoid issues with overlapping categories, for example attending a business event to talk with end-user SME.
- 'Downloads form the PRIViLEDGE website' is removed as a separate category as all information on website can be seen without downloading, including deliverables and scientific publications. Website visitors is used to make sure project website is relevant.
- 'Press/general articles' category is replaced with news items.
- 'Blogpost' category because as PRIViLEDGE is a research project, general media articles are difficult to publish during the project development.
- 'Press releases' are not considered as a KPI as news, social media and blog posts can be also published or shared on various websites. Press releases might still be used when relevant.

KPI	Planned M13-M24	Adjusted M13-M24	Planned M25-M36	Adjusted M25-M36	Total M1-M26	Comments
Events attended representing the project	15	15	20	20	50	The project partners will continue to attend various scientific and industry related events.
Business/industry events and communication	-	25	-	35	80	This category includes communication with SMEs, relevant industry and end-users.
Academic events and communication	-	25	-	25	70	This category includes scientific conferences, workshops, research collaborations.
Publications in peer-reviewed journals and conferences	4	4+	4	4+	13	The first year indicated that the scientific level of the work is very high.
Blogposts	-	12	-	12	24	A new blog entry will be published every month on the website and linked on partner's sites. The schedule is available in Table 2.
News on website	-	4	-	4	10	News will be updated at least quarterly to share important progress or event information.
Workshops of the project	3	2	1	2	4	The original plan was to have 3 workshops during the second year, however, as the latter two workshops will be focussed on results from the use-cases, the best time for them is on the final year.
Website visitors	6000	6000	10000	9000	17000	Although the visitor numbers were lower than planned for year one, a significant increase is expected with more posts and organised workshops.
Mentions of PRIViLEDGE in other websites	15	15	20	20	50	PRIViLEDGE mentions are expected to be about organised workshops; presentations at conferences, seminars, and summer schools; blog posts and news published on the project website shared or mentioned on various channels.
Followers on social media (Twitter)	250	250	350	350	350	In next years, more information will be available through Twitter and therefore a significant increase is expected with every workshop.

Table 3: KPIs for M13-M36

Appendix A Twitter Plan

PRIViLEDGE Twitter plan

Tuuli Lõhmus (GT)
tuuli.lohmus@guardtime.com

November 2018

Abstract

This document provides a short guideline for using Twitter @*PRIViLEDGE_EU* throughout the PRIViLEDGE project and engaging with the handle to ensure widest visibility and dissemination of results.

1 Posting in Twitter

1.1 Social media post guidelines

- Use short and direct language aimed at wide audience
- Link to more information and publications
- Use graphics, videos and images for context
- Engage with scientists, community, stakeholders and journalists for greater visibility
- Promote project values as well as results and activities
- use @*EU_H*2020 and #H2020 to maximise their visibility

1.2 Formatting and choosing keywords

1.2.1 Language and format

By nature, Twitter limits characters to 280 per post. Therefore, the language of the posts has to be concise. The emoticons should be used to illustrate the point, draw attention to keywords, or share emotions.

1.2.2 Keywords

Keywords are used to link posts to a specific topic. They can be used below the message or inside the text. Keywords are chosen for each post according to its content. Examples of some common keywords are given below.

Specific keywords

#cryptography, #security, #privacy, #blockchain, #smartcontracts, #decentralization, #DLT

General keywords

#H2020, #knowledge, #equality, #science, #workshop

2 Engaging in Twitter

2.1 Promoting project events and results

Twitter platform should be used to promote project results by sharing the latest news or published papers. Moreover, all upcoming events what PRIViLEDGE is attending or hosting are shared on Twitter to ensure wide visibility and link to detailed information at the project website.

2.2 Engaging with specialist community and wider audience

Twitter community is first identified by following cryptography, distributed ledger technology and blockchain developers and stakeholders. Retweeting and liking interesting content enhances project timeline so people see both the results and wider context for them. Interesting and informative timeline encourages others to follow the project. Another main way to reach both specialist community and wider audience is retweeting project posts. All partners are strongly encouraged to share relevant content about events, publications and events on their Twitter pages. Sharing and following with comments provides a direct connection with project audience.

2.3 Sharing outside content

Sharing outside content makes project more visible and well-balanced. There are some guidelines how to determine if the content should be shared based on who is sharing it and how it relates to the project. This is not an exhaustive list but some ideas for educational and fact-based timeline.

2.3.1 Who is sharing it?

There are a number of accounts that are often posting relevant content by

- EU official account
- Project partner official account
- Project partner personal account
- Well-established company or newspaper
- Scientific institution or publication
- Another H2020 project
- Expert or student in a field
- ...

The project account will never interact with provocative messages or personal attacks.

2.3.2 How it relates to project?

To keep the Twitter feed interesting and relevant to the project, content is evaluated before sharing. Below are some ideas how to determine if the content is relevant:

- Posts relevant to project topic - e.g. cryptography, DLT, blockchain news and developments
- Posts about talks, workshops, presentations where project partners are attending or presenting - e.g. sharing university course or seminar info
- European Commission and H2020 relevant news
- General discussions on privacy, cybersecurity, importance of science and technology