DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

D5.1 – Initial Communication and Dissemination Plan

Due date of deliverable: 30.06.2018
Actual submission date: 29.06.2018

Grant agreement number: 780477
Start date of the 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	

D5.1

Initial Communication and Dissemination Plan

Editor
Mirjam Kert (GT)

Contributors
Ahto Truu (GT)

Reviewers
Björn Tackmann (IBM), Ivan Visconti (UNISA)

29.06.2018
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.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Contents

1 Introduction

In addition to the core activities of the project, 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 initial Communication and Dissemination Strategy of PRIViLEDGE and is central to all activities that will be implemented towards relevant stakeholders and interested parties.

The Plan for Dissemination and Communication defines the identification and classification of the target audience, the dissemination methods and goals, the measures to assess the impact of the dissemination activities, and the conditions to follow to ensure proper dissemination of the generated knowledge with regards to confidentiality, publication, and use of the knowledge.

2 Strategy for Dissemination and Communication

2.1 Purpose

The overall aim of the dissemination activities outlined below is to ensure generating impact through engagement with the stakeholders in the ecosystems that benefit most from the results of the project. For this purpose, the Plan for Dissemination and Communication will ensure that the project research and practical outcomes are widely disseminated to the appropriate target audiences at appropriate times along the project lifecycle.

The objectives of the communication and dissemination activities are:

- 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.

Dissemination activities will address raising awareness and getting the necessary feedback, as well as building understanding and facilitating adoption of project 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.

The objectives of the dissemination and communication activities will be mainly deployed in stages during the project lifetime. In addition to the central objective specified above, other objectives will be targeted in these stages as follows:

- **Stage 1 (M1-M12):** Raising general awareness of project activities, outputs and benefits through diverse channels to audiences.
- **Stage 2 (M12-M24):** Promoting a deeper understanding of new knowledge and results for a number of audiences who can benefit from what PRIViLEDGE project can offer.
- **Stage 3 (M25-M36):** Engaging with target groups to encourage their willingness to make use of project results. Influencing decision-making within organisations regarding the uptake of PRIViLEDGE outputs and supporting the implementation of the Exploitation Plan.

2.2 Key Messages

The message component of the dissemination and communication strategy comprises of the set of arguments, reasons and facts to be used to convince 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 a primary key message and 5 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 payment, leveraging tools such as privacy-preserving mechanisms and quantum-safe cryptography, while focusing on the emerging distributed ledger technology."*
- *"PRIViLEDGE shows how to perform practical, secure and privacy-protecting 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".*

2.3 Target Audiences

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.

Target group	Media	Goal of dissemination
Industry: e-voting, insurance, higher education, systems management, other applicable sectors	Existing business relationships, policy reports, meetings, conferences, seminars/ workshops, meet-ups	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	Existing business relationships, policy reports, meetings, conferences, seminars/ workshops, meet-ups	To engage them in the up-take of innovation that PRIViLEDGE produces.

Research and scientific community	Academic publications, journals, conferences, workshops	To engage them in dialogue, to present them research results and ignite further academic work.
Public sector	Policy reports, meetings, conferences, workshops, social media	To engage them in the relevant research for their purposes such as the e-voting use case that PRIViLEDGE will develop.
General public	Policy reports, meetings, conferences, workshops, social media	To engage the public in a debate on security and privacy.

2.4 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 will be used in all the dissemination outputs, such as the project website, social media accounts, the project videos and leaflets, etc.

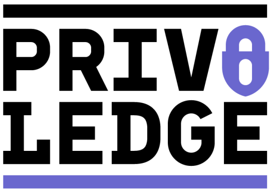

Figure 1: The PRIViLEDGE logo

2.5 Description to be Used in External Communication and Tags

The following tags are suggested for online communications (depending on the specific publication topic), for example as hashtags for Tweets:

#cryptography, #security, #privacy, #crypto #blockchain, #cryptocurrencies, #smartcontracts, #decentralization

PRIViLEDGE will be described in a coherent way to the outside world. The following text shall be used when describing the project on their institutional websites, in newsletters, etc. Variations for different target groups are possible.

The PRIViLEDGE project aims to develop cryptographic protocols supporting privacy, anonymity, and efficient decentralised consensus for distributed ledger technologies/blockchains. In PRIViLEDGE, several European key players in cryptographic research and from the fintech and blockchain domains unite to push the limits of cryptographic protocols for privacy and security. To show concrete examples of the validity of the developed technology four ledger-based use cases have been chosen: (1) verifiable online voting; (2) contract validation and execution for insurance; (3) university diploma record ledger; and (4) update mechanism for stake-based ledgers. The selected use cases are diverse and represent the principal application domains of DLT; this ensures wide reach and impact of the techniques developed in PRIViLEDGE beyond the immediate scope of the project.

2.6 Management

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).

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 will be uploaded and maintained on GitHub. Roles of participants in communication and dissemination activities:

GT: As an industrial lead for the project and responsible party for Communication and Dissemination, Guardtime coordinates the communication and outreach activities. Guardtime will also present PRIViLEDGE at conferences, workshops and industrial trade shows.

Guardtime will organise workshops communicating key research results, the main results of the use cases. Guardtime will distribute all the policy recommendations relating to standardisation activities and other outcomes of the project with the aim of reaching the target audiences and insertion into relevant documents. Guardtime will use its existing business network as well as its Vice-Chairmanship at the European Cyber Security Organisation (ESCO) to make sure all the necessary information reaches the most relevant public authorities as well as the most relevant European and international industry.

IBM: As an industry research lab, IBM Research - Zurich uses various channels to communicate results. IBM publishes research papers at leading scientific venues. The communications team of IBM Research - Zurich supports dissemination of results using contacts to the media, through press releases, the lab web site, or social media. Examples of this from the past include regularly occurring announcements of novel technology capabilities (see http://www.zurich.ibm.com/news/). IBM regularly uses technology innovation from IBM Research for building technology and for its service engagements. The close dialogue between customers, business units, and research has two beneficial effects: First, it aligns the research to the demands of the market and ensures that the research effort is aware of the requirements from the customers' side. Complementing this as a second force, insight from research, early technology previews, and feasibility studies are regularly influencing the business side. Finally, IBM is a member of (industry) associations in the relevant area such as the Hyperledger Project or the IC3 initiative for CryptoCurrencies and Contracts, and regularly contributes to standardisation processes at IETF, OASIS, ISO, SOVRIN and many more.

UT: As an academic partner, UT will disseminate the project work mainly by publishing in leading cryptography and data security conferences. On top of that, UT expects to publish on specialised conferences on topics related to this project; this includes the Financial Cryptography conference together with its workshops and various conferences and promotional events on e-voting.

UEDIN: As an academic partner, UEDIN will engage with the research community in the broad area of cybersecurity, cryptography and distributed systems. Particular venues of interest include ACM CCS, the Asiacrypt, Crypto, and Eurocrypt conferences, IEEE S&P, ESORICS, ACM Symposium on Applied Computing (SAC), Annual Computer Security Applications Conference (ACSAC), ACM Workshop on Privacy in the Electronic Society (WPES), Workshop on Privacy Enhancing Technologies, IEEE Computer Security Foundations Workshop (CSF). Finally, FC together with its satellite workshops, on BITCOIN

Research and Smart Contracts will be particularly suited for connecting with the international community in the area of distributed ledgers. A number of journals will also be considered, including but not limited to, ACM Transactions on Information and System Security, Computers & Security, IEEE Security and Privacy Magazine, IIE Transactions, International Journal of Applied Cryptography, International Journal of Information Security, Journal of Computer Security, Journal of Cryptology.

TUE: Apart from communicating the project results through scientific and academic channels, TUE intends to strengthen its links with Dutch industry (Philips) and government agencies (TNO, CBS). Currently, TUE is in touch with these organisations about practical use of secure multiparty computation. Because of PRIViLEDGE, TUE intends to include the use of distributed ledgers in its communications with these organisations.

UNISA: Members of the team will work for the dissemination of the results of the project. They will promote through an active plan the renovated importance of defending user privacy from the fast, uncontrolled growth of distributed ledgers. In addition to scientific publications, annual press releases and various announcements will be used by members of the team to communicate the high impact of PRIViLEDGE towards obtaining constructions of robust and effective distributed ledgers.

SCCEIV: SCCEIV publishes results of its works regularly. Venues of interest are conferences and journals that are focused on the topic of electronic and online voting—The International Conference for Electronic Voting (E-Vote-ID) and Financial Cryptography and Data Security Workshop on Advances in Secure Electronic Voting Schemes.

GRNET: Even though GRNET is an industrial partner, it has a continuous presence in the research community, specifically in the area of cybersecurity and privacy, and software engineering. Venues of interest include high impact journals like ACM TOPS, IEEE TDSC, and Computers & Security, together with top-tier conferences like Usenix Security, ACM CCS, IEEE S&P, ICSE, and EuroSys.

GUNET: GUNET will make sure that necessary information, including the prerequisites of online connection of Student Information Systems with the Diplomas Ledger, will reach Greek universities via the organisation of local workshops. The results of PRIViLEDGE will also be communicated in these workshops. In addition to that, the project results will be communicated in relevant conferences and journals in the area of interoperability and university Information Systems, such as European University Information Systems (Eunis).

3 Communication and Dissemination Channels

PRIViLEDGE will utilise multiple communication channels to be as interactive as possible in order to stimulate interest and target global, European, and local markets/communities. To reach out to relevant stakeholders, PRIViLEDGE will utilise online and offline communication channels and organise events and workshops. In addition to creating specific communication materials, the project will also use the existing networks of participants to increase its visibility and impact and to gather valuable feedback. The project website is the primary information source for target stakeholders. Open access to scientific publications is also important to the consortium, and in particular to the academic partners. The PRIViLEDGE consortium believes that social media is a good means of outreach to the public permitting bidirectional communication. Last but not least, consortium partners are actively participating in external events and in the organisation of four project workshops.

3.1 Online Communication

3.1.1 Website

The main PRIViLEDGE dissemination channel is its official website (www.priviledge-project.eu), presenting the project and its on-going activities as well as key results and outputs. The website is designed in a way to guarantee a high level of accessibility and usability. The website is currently divided in to 5 sections, an “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, also introducing the Advisory Board. The third section consists of project deliverables and publications which have been produced. News and news archives are included under the “News” section. The final section “Contact” consists of the Coordinator contact. The website is also linked to Twitter.

The structure, language and style that we use in this website is in line with that used in similar EU-funded projects. We foresee that the website will be one of the main entry points to the project.

3.1.2 Social Media

Due to the wide popularity of social media, the project members have decided to set up social media accounts for the project. The purpose of those accounts is to reach wide and targeted audiences in a fast and efficient manner. Social media will be 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.

The PRIViLEDGE project will mainly use one social media channel: Twitter. A separate PRIViLEDGE account has been created in Twitter (https://twitter.com/PRIViLEDGE_EU). Twitter will be used for sharing short messages, making announcements and retweeting relevant messages. The project partners help to enhance the project outreach by retweeting. The PRIViLEDGE Twitter account will be used to inform the broader European cybersecurity community and the wider public about the project's objectives and technical developments as they occur. A specific Twitter plan will be developed by Guardtime and shared with the rest of the Consortium, to coordinate the activities of the partners and guarantee a coherent approach.

3.2 Offline Materials

Formal academic publishing: PRIViLEDGE project research results will be published in the main peer-reviewed journals and conferences with formal proceedings.

Informal academic presentations: 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, will be used to present the research results of PRIViLEDGE.

Business presentations: 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.

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 results will also be transferred to the different ECSO working group activities and to the policy makers.

General publishing: Various general articles will be produced for dissemination to different target audiences via journals such as Security Europe, ACM Transactions on the Web and IEEE Internet Computing.

COST Action: PRIViLEDGE consortium members are a part of a COST (http://www.cost.eu/) action application on blockchain technology and are actively seeking for further collaboration with academic partners.

Promotional material: A brochure, poster, and special template design for presentations will be created which will give an overview of the project.

3.3 Events

The PRIViLEDGE events will come as a dissemination support to the objectives of WP5. They will help in spreading the project outputs to the respective target audiences, facilitate valuable feedback from respective stakeholders, and provide ground for discussion and brainstorming.

The project will have 4 dedicated workshops throughout three years:

- **Workshop 1:** dedicated to deliver PRIViLEDGE research results in the second half of the project when results can be presented;
- **Workshop 2:** 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;
- **Workshop 3:** dedicated to exploitation of PRIViLEDGE results; the objective is to perform expert interviews and focus groups;
- **Workshop 4:** 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.

Additionally, the PRIViLEDGE project aims to exhibit its results in various conferences by having a special exhibition area, communicating via dedicated panels, and presentations. Currently PRIViLEDGE project in cooperation with the FENTEC project (http://fentec.eu/) has applied for a joint exhibition area at ICT2018. In the future we are also interested in participating in events like Annual Privacy Forum and other events organised by the European Commission.

4 Open Access

PRIViLEDGE will 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 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 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.

5 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) have been identified. The KPIs of the PRIViLEDGE project's communication and dissemination activities are planned and indicated in the Description of Action.

KPI for Dissemination & Communication	**Phase 1** **M1-12**	**Phase 2** **M13-24**	**Phase 3** **M25-36**	**Total**
Events attended representing the project (including conferences and workshops)	10	15	20	45
Business events attended	3	5	5	13
Communication with SMEs	10	10	10	30
Communication with other relevant industry	5	10	20	35
Communication with end users	10	20	30	60
Publications in peer-reviewed journals and conferences	1	4	4	9
Press/general media articles published	5	10	10	25

Workshops of the project	0	3	1	4
Press releases	5	5	10	20
Website visitors	3000	6000	10000	19000
Mentions of PRIViLEDGE in other websites	10	15	20	45
Downloads from PRIViLEDGE website	200	400	800	1400
Followers on social media	100	250	350	700