



DS-06-2017: Cybersecurity PPP: Cryptography

PRIVILEGE

Privacy-Enhancing Cryptography in Distributed Ledgers


D6.1 – Project Reference Manual and Tools

Due date of deliverable: 31 March 2018

Actual submission date: 31 March 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 | | |

D6.1

Project Reference Manual and Tools

Editor

Mirjam Kert (GT)

Contributors

Ahto Truu(GT)

Reviewers

Björn Tackmann (IBM), Aggelos Kiayias (UEDIN)

31 March 2018

Revision 1.0

The work described in this document has been conducted within the project PRIVILEGE, 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.

©Copyright by the PRIVILEGE Consortium

Contents

| | | |
|-----|---|----|
| 1 | Objective of the deliverable | 2 |
| 2 | Project Basis..... | 2 |
| 2.1 | Project Participants and Contacts..... | 2 |
| 2.2 | Contractual Documents..... | 3 |
| 2.3 | Grant Agreement (EC-GA) | 3 |
| 2.4 | Consortium Agreement (CA)..... | 3 |
| 3 | Project Structure..... | 3 |
| 3.1 | Work Packages..... | 3 |
| 3.2 | Deliverables | 5 |
| 3.3 | Milestones | 6 |
| 4 | Project Management | 6 |
| 4.1 | Project Structure | 6 |
| 4.2 | Conflict Resolution | 9 |
| 4.3 | Contractual Management..... | 9 |
| 4.4 | Administrative and Financial Reporting to EC..... | 10 |

1 Objective of the deliverable

The object of deliverable D6.1 – Project Reference Manual and Tools is to provide:

- Guidelines for management of procedures and reporting
- Overview of the project basis

Along with D6.2 – Quality Assurance Plan, the two documents aim to give a full overview on the PRIViLEDGE project management processes.

2 Project Basis

2.1 Project Participants and Contacts

Official contact information for each of the Project Participants is included in the EC-GA of the project. The project list of partners is the following:

| NO. | ORGANISATION NAME | SHORT NAME | Participant type | COUNTRY |
|--------|---|------------|------------------|----------------|
| 1 (PC) | GUARDTIME AS | GT | Industry | Estonia |
| 2 | IBM Research - Zurich | IBM | Industry | Switzerland |
| 3 | University of Tartu | UT | Academia | Estonia |
| 4 | University of Edinburgh | UEDIN | Academia | United Kingdom |
| 5 | Technical University of Eindhoven | TUE | Academia | Netherlands |
| 6 | University of Salerno | UNISA | Academia | Italy |
| 7 | Smartmatic-Cybernetica Centre of Excellence for Internet Voting | SCCEIV | Industry | Estonia |
| 8 | Greek Research and Technology Network | GRNET | Industry | Greece |
| 9 | Greek Universities Network | GUNET | Industry | Greece |

TABLE 1: PARTNERSHIP TABLE

The duration of the project is 36 months. The starting date of the project is 1st of January 2018 and the finishing date 31st December 2020. The project has an overall budget of 4,527,917.50€. The budget of the project, as well as its distribution between the Members of the Consortium, is detailed in EC-GA, Annex I and II.

The EC contribution for each partner is a maximum contribution conditioned to the acceptance by the EC of expenses up to budget of the partner. This means that if a partner spends less than what was approved in their budget (or the EC does not accept all their costs), they will only receive the proportional part of the EC contribution.

D6.1 – Project Reference Manual and Tools

2.2 Contractual Documents

The reference documents for the project Consortium members, which define their tasks, rights and obligations are the EC-GA (including its annexes) and the CA (including its addendums if any).

2.3 Grant Agreement (EC-GA)

The Grant Agreement with the EC: EC-GA No. 780477 is the contractual document signed by all the project partners which defines the rights and the obligations of the Consortium with the EC. The EC-GA includes the following annexes:

- EC – GA Annex 1 – Description of Action (DoA): This the contractual document which describes the work to be performed by the project Consortium.
- EC – GA Annex 2 – Estimated budget for the action: This Annex describes the general budget and every partner’s budget per cost category.
- EC – GA Annex 2a – Additional information on the estimated budget
- EC – GA Annex 3 – Accession forms
- EC – GA Annex 4 – Model for the financial statement
- EC – GA Annex 5 – Model for the certificate on the financial statements (CFS)
- EC – GA Annex 6 – Model for the certificate of the methodology

2.4 Consortium Agreement (CA)

The Consortium Agreement (CA) is the internal contract of the consortium partners which has been signed and accepted by all partners. It defines the consortium internal rules for project management as well as the consortium organization and decision mechanisms. In case of discrepancy, the CA is overruled by the EC-GA.

3 Project Structure

The work carried out in PRIViLEDGE must follow the DoA, schedule and budget defined in the EC-GA of the project (Annex I – Description of Action). The project and work organization is mainly defined by the project WPs and deliverables.

3.1 Work Packages

The WP structure and WP interactions, as defined in the Description of Action, are the following:

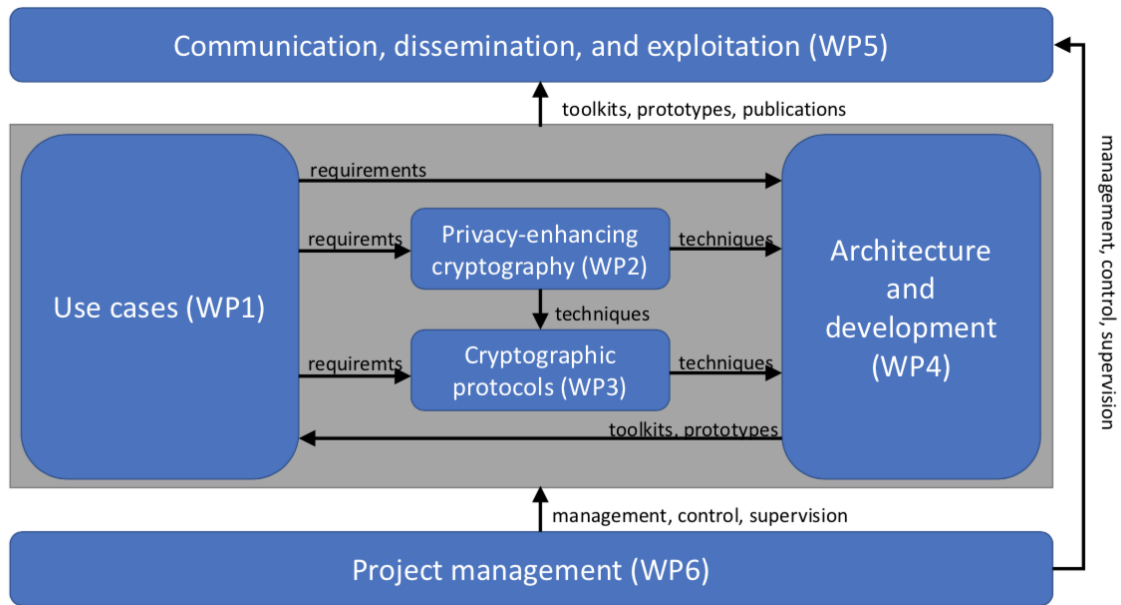


FIGURE 2: WP STRUCTURE

The detailed description of each of the WPs can be found in the EC-GA, Annex I (Description of Action).

The main characteristics of each WP in which the project has been structured are the following:

| Work Package | Work Package title | Lead Partic. Short Name | Person Months | Start Month | End Month |
|--------------|--|-------------------------|---------------|-------------|-----------|
| WP1 | Use cases | GRNET | 68 | M1 | M36 |
| WP2 | Privacy-enhancing cryptography | UNISA | 112 | M1 | M36 |
| WP3 | Cryptographic protocols | TUE | 131 | M1 | M36 |
| WP4 | Architecture and development | IBM | 129 | M7 | M36 |
| WP5 | Communication, dissemination, and exploitation | GT | 62 | M1 | M36 |
| WP6 | Project management | GT | 26 | M1 | M36 |
| | TOTAL | | 528 | | |

FIGURE 3: WP EFFORT AND DURATION

Each work package will have a work package leader (WPL), who will have the responsibility and serve as the contact person for that work package. WP leaders will be responsible for organising and managing the work within the individual work packages, including detailed planning of tasks and activities, the technical solution, the persons responsible for specific activities and the control of results from the activities. In addition, they will provide deliverables against milestones and other reporting required.

D6.1 – Project Reference Manual and Tools

3.2 Deliverables

The list of deliverables for the 36 months of the project is shown below. Each of the deliverables must be finished and submitted to the EC at the latest on the date shows in the table below. In case a delay is foreseen, it should be reported to PC by the WP leader, who will apply the necessary corrective actions and inform the EC officer if necessary.

| Del. No. | Deliverable Name | Work Package | Lead Partic. | Nature | Dissem. Level | Delivery Month |
|----------|---|--------------|--------------|--------|---------------|----------------|
| D1.1 | Requirements and Interface Design | WP1 | GRNET | R | PU | 12 |
| D1.2 | Validation Criteria | WP1 | UEDIN | R | PU | 30 |
| D1.3 | Use Case Validation | WP1 | SCCEIV | R | PU | 36 |
| D2.1 | State of the art on Privacy-Enhancing Cryptography for Ledgers | WP2 | UT | R | PU | 6 |
| D2.2 | Definitions and Notions of Privacy Enhancing Cryptographic Primitives for Ledgers | WP2 | UNISA | R | PU | 30 |
| D2.3 | Improved Constructions of Privacy – Enhancing Cryptographic Primitives | WP2 | UNISA | R | PU | 30 |
| D2.4 | Revision of Privacy – Enhancing Cryptographic Primitives for Ledgers | WP2 | UT | R | PU | 36 |
| D3.1 | State of the Art of Cryptographic Ledgers | WP3 | UEDIN | R | PU | 8 |
| D3.2 | Design of Extended Core Protocols | WP3 | TUE | R | PU | 24 |
| D3.3 | Revision of Extended Core Protocols | WP3 | UEDIN | R | PU | 36 |
| D4.1 | Report on Architecture of Secure Ledger Systems | WP4 | UEDIN | R | PU | 18 |
| D4.2 | Report on Aechitecture for Privacy-Preserving Applications on Ledgers | WP4 | GRNET | R | PU | 24 |
| D4.3 | Final report on Architecture | WP4 | IBM | R | PU | 30 |
| D4.4 | Report on Tools for Secure Ledger Systems | WP4 | IBM | R | PU | 36 |
| D4.5 | Report on Tools for Privacy-Preserving Applications on Ledger | WP4 | GT | R | PU | 36 |
| D5.1 | Initial Communication and Dissemination Plan | WP5 | GT | R | PU | 6 |
| D5.2 | Communication and Dissemination Toolkit | WP5 | GT | R | PU | 9 |

D6.1 – Project Reference Manual and Tools

| | | | | | | |
|------|---|-----|-----|---|----|----|
| D5.3 | Exploitation Strategy and Roadmap | WP5 | IBM | R | PU | 9 |
| D5.4 | Updated Consolidated Communication and Dissemination Plan | WP5 | GT | R | PU | 12 |
| D5.5 | Report on Exploitation | WP5 | IBM | R | PU | 33 |
| D5.6 | Stakeholder Engagement Report | WP5 | GT | R | PU | 36 |
| D6.1 | Project Reference Manual and Tools | WP6 | GT | R | PU | 3 |
| D6.2 | Quality Assurance Plan | WP6 | IBM | R | PU | 3 |
| D6.3 | First Scientific & Research Impact Measurement | WP6 | IBM | R | PU | 18 |
| D6.4 | Second Scientific & Research Impact Measurement | WP6 | IBM | R | PU | 36 |

Each work package leader is responsible for the organisation of the deliverables for their work package, including internal review of all reports. Once a report has passed internal work package review, it must pass project-level review. The Project Coordinator and Scientific Coordinator may review any deliverables before submission and may return them for additional refinement if they find this necessary.

3.3 Milestones

The list of milestones of the project is the following:

| Milestone | Due | Description |
|---|-----|----------------------------|
| MS1: Project successfully started | M3 | D6.1, D6.2 completed |
| MS2: State of the art | M8 | D2.1, D3.1 completed |
| MS3: Requirements for all use cases defined | M12 | D1.1 completed |
| MS4: Design of core primitives | M24 | D.2.2, D3.2 completed |
| MS5: Architecture and validation criteria finalised | M30 | D1.2, D4.3 completed |
| MS6: Tools and use cases developed and validated | M36 | D1.3, D4.4, D4,5 completed |

4 Project Management

4.1 Project Structure

PRIViLEDGE is a research project with 7 Work Packages (WPs) and 10 partners, coordinated by Guardtime AS. IBM Research will act as the technical leader and will be responsible for the scientific coordination of the project. In more detail, the partners involved in the project are:

1. Guardtime AS (GT, Estonia, industry), Coordinator
2. IBM Research – Zurich (IBM, Switzerland, industry)
3. University of Tartu (UT, Estonia, academia)

D6.1 – Project Reference Manual and Tools

4. University of Edinburgh (UEDIN, United Kingdom, academia)
5. Technical University Eindhoven (TUE, Netherlands, academia)
6. University of Salerno (UNISA, Italy, academia)
7. Smartmatic-Cybernetica Centre of Excellence for Internet Voting (CEIV, Estonia, industry)
8. Greek Research and Technology Network (GRNET, Greece, industry)
9. Greek Universities Network (GUNET, Greece, industry)

The interaction, responsibilities and decision-making power is clearly divided between the established project bodies as described in the following. The governing culture of the PRIViLEDGE project is based on collective decision-making, co-determination and clear leadership.

Key roles. *The Project Coordinator (PC)* ensures the overall coordination including daily supervision and monitoring of operations and official communication with the European Commission and with other parties, such as other relevant EU and national projects, relevant bodies and other related activities. The Project Coordinator is Mari Kert-Saint Aubyn from GT. *The Scientific Coordinator (SC)* has the overall responsibility of ensuring content synchronisation between the different PRIViLEDGE outcomes, as well as alignment to the overall PRIViLEDGE goals. The SC is Christian Cachin from IBM. *The Innovation Manager (IM)* is responsible for linking with industry beyond the consortium. The IM is Ivo Löhmus from GT.

General Assembly. *The General Assembly (GA)* is the highest decision making board and its main task is project governance. It consists of one representative of each partner, is chaired by the Project Coordinator and convenes at least once a year. The following representatives and deputies have been defined to present their organization within the PRIViLEDGE General Assembly:

- GT: Mari Kert-Saint Aubyn, deputy: Mirjam Kert
- IBM: Christian Cachin, deputy: Björn Tackmann
- UT: Helger Lipmaa, deputy: Michał Zając
- UEDIN: Aggelos Kiayias, deputy: Vassilis Zikas •
- TUE: Berry Schoenmakers, deputy: Niels de Vreede
- UNISA: Ivan Visconti, deputy: Giuseppe Persiano
- SCCEIV: Sven Heiberg, deputy: Ivo Kubjas
- GRNET: Panos Louridas, deputy: Georgios Tsoukalas

D6.1 – Project Reference Manual and Tools

- GUNET: Nikos Voutsinas, deputy: Spiros Bolis

Project Management Committee. *The Project Management Committee (PMC)*, led by the Project Coordinator, is the executive body of the project and will meet face-to-face or by teleconference at least every three months, or as required. The Project Management Committee will comprise one representative from each partner, the PC and the SC. The PMC reports to the General Assembly.

- PC: Mari Kert–Saint Aubyn (GT, chair)
- SC: Christian Cachin (IBM)
- GT: Mirjam Kert, deputy: Ahto Truu
- IBM: Björn Tackmann, deputy: Angelo De Caro
- UT: Helger Lipmaa, deputy: Michał Zaja ę
- TUE: Berry Schoenmakers, deputy: Niels de Vreede
- UNISA: Ivan Visconti, deputy: Giuseppe Persiano
- CEIV: Sven Heiberg, deputy: Ivo Kubjas
- GRNET: Panos Louridas, deputy: Georgios Tsoukalas
- GUNET: Nikos Voutsinas, deputy: Spiros Bolis
- UEDIN: Aggelos Kiayias, deputy: Vassilis Zikas

Technical Management Committee. *The Technical Management Committee (TMC)* has the assignment of ensuring the timely progress of the project and the high quality of the results. The TMC reports to the PMC. It will meet (either face to face or by teleconference) every month and once at the end of the project to review the success of the project. The TMC will be chaired by the SC. The leaders of all work packages (WPs) will be members, along with the PC.

- SC: Christian Cachin (IBM, chair)
- PC: Mari Kert-Saint Aubyn (GT)
- WP1: Panos Louridas (GRNET), deputy: Ahto Truu (GT)
- WP2: Ivan Visconti (UNISA), deputy: Helger Lipmaa (UT)
- WP3: Berry Schoenmakers (TUE), deputy: Aggelos Kiayias (UEDIN)
- WP4: Björn Tackmann (IBM), deputy: Angelo De Caro (IBM)
- Work packages 5, 6, and 7 are lead by GT.

Advisory Board. The PRIViLEDGE project is in the process of establishing a focused, industry-driven Advisory Board (AB), in order to discuss and agree upon marketing and

D6.1 – Project Reference Manual and Tools

innovation stimuli as well as research directions. The PRIViLEDGE advisory board will be contacted regularly during the project to provide guidance to the project.

4.2 Conflict Resolution

In the event of major conflict occurring between two or more partners, the following actions are proposed:

- As a general rule, project management will aim at consensus building, promoting mediation over voting in order to ensure a maximum degree of cooperation within the consortium.
- Attempts will be made to resolve conflicts as close as possible to the source of the conflict. That is, conflicts within a WP will be managed by the WP leader. If conflicts cannot be resolved at that level, the PMC will be asked to intervene. The GA is the ultimate level to intervene in the conflict-resolution chain.
- The PC can play the role and assume the authority of arbitrator if accepted unanimously by all parties involved in the conflict about a specific matter.
- Important decisions on different issues, technical or otherwise, pertaining to the overall project will be reached by consensus decision-making in the PMC, if necessary by asking for the advice of external experts.

4.3 Contractual Management

The objective of contractual management is to ensure the project is adhering to the terms and conditions of the Grant Agreement (the contract with the European Commission) and providing the required services/products that meet the expectations of the project. In particular the contract management addresses the following situations:

- Changes in the consortium configuration, such as addition or withdrawal of beneficiaries or third parties. •
- Changes in in the technical scope of the project, affecting the Description of Action (DoA).
- Changes in the Consortium Agreement.
- Contract closing.

Contractual changes are decided at the GA level in accordance to the procedures set out within the CA and the article 55 of the Grant Agreement (except in the case of change of coordinator). The PMC can also propose changes to the GA. Any changes to the project plan and scope must be reviewed and approved by all levels of project management, before

D6.1 – Project Reference Manual and Tools

proposing these changes to the GA and any modification will be considered rejected, after rejection on any of these involved levels. The PC is in charge of processing and coordinating any amendment on behalf of the consortium. The PC is also responsible for transferring any contractual change to the project plan.

4.4 Administrative and Financial Reporting to EC

The European Commission contract sets out some mandatory requirements for reporting:

- Deliverables: identified in the list of deliverables included in the Grant Agreement.
- Periodic report: as described in Article 20.3 of the Grant Agreement, within 60 days from the end of each reporting period (including the last one). In PRIViLEDGE there are two reporting periods (RP):
 - RP1: from month 1 (January 2018) to month 18 (June 2019) 4
 - RP2: from month 19 (July 2019) to month 36 (December 2020)
- These periodic reports shall include:
 - A periodic technical report containing:
 - An explanation of the work carried out by the beneficiaries;
 - An overview of the progress towards the objectives of the action, including milestones and deliverables identified in the DoA.
 - A summary for publication by the EC.
 - The answers to the “questionnaire”, TO BE COMPLETED covering issues related to the action implementation and the economic and societal impact, notably in the context of the Horizon 2020 key performance indicators and the Horizon 2020 monitoring requirements;
 - A periodic financial report containing:
 - An individual financial statement (drafted in euros) from each beneficiary and from each linked third party, for the reporting period concerned.
 - An explanation of the use of resources and the information on subcontracting and in-kind contributions provided by third parties from each beneficiary and from each linked third party, for the reporting period concerned;
 - A periodic summary financial statement, created automatically by the EC Participant Portal electronic exchange system.

D6.1 – Project Reference Manual and Tools

- Final report: within 60 days after the end of the project. The final report should include:
 - A final technical report with a summary for publication containing: an overview of the results and their exploitation and dissemination; the conclusions on the action; and the socio-economic impact of the action;
 - A final financial report containing:
 - A final summary financial statement (in euros) created automatically by the electronic exchange system, consolidating the individual financial statements for all reporting periods and including the request for payment of the balance.
 - A certificate on the financial statements (CFS) for each beneficiary and for each linked third party, if it requests a total contribution of EUR 325,000 or more, as reimbursement of actual costs and unit costs calculated on the basis of its usual cost accounting practices.