# PRIV LEDGE

DS-06-2017: Cybersecurity PPP: Cryptography

PRIViLEDGE
Privacy-Enhancing Cryptography in Distributed Ledgers

## D6.2 – Quality Assurance Plan

Due date of deliverable: 31 March 2018
Actual submission date: 31 March 2018

Grant agreement number: 780477
Start date of project: 1 January 2018
Revision 1.1

Lead contractor: Guardtime AS
Duration: 36 months

# D6.2

# Quality Assurance Plan

**Editor**
Björn Tackmann (IBM)

**Contributors**
Christian Cachin (IBM)

**Reviewers**
Mirjam Kert (Guardtime), Panos Louridas (GRNET)

31 March 2018
Revision 1.1

## Executive Summary

This Quality Assurance Plan shows how quality aspects are taken into account in a variety of processes and activities within the PRIViLEDGE project. The interrelated quality processes—planning, assurance and control—are outlined in this document. Hereby, quality planning refers to defining quality policies and creating necessary tools such as a common visual identity or templates for documents. Quality assurance involves defining clear responsibilities and keeping all work packages and partners of the project connected through reports as well as regular meetings and teleconferences. Quality control, finally, focuses on feedback through internal deliverables and review processes, as well as the advisory board. The Quality Assurance Plan is an integral part of the project management.

The plan is effective throughout the lifetime of the project, but is open to revision if necessary. Responsibilities for quality planning, assurance and control are shared between all partners, which allow various views on quality issues in order to reach the optimal outcome.

# Contents

# 1  Introduction

The Quality Assurance Plan is an integral part of the PRIViLEDGE project management. Its purpose is to describe how quality will be managed throughout the lifecycle of the project. Quality must always be planned in a project in order to prevent unnecessary rework, as well as waste of cost and time. Quality should also be considered from both an outcome and process perspective. The processes and activities that produce deliverables need to fulfill certain quality levels in order to reach the expected high-quality outcome. To address all quality requirements and quality assurance mechanisms in the PRIViLEDGE project, the *Quality Assurance Plan* at hand has been developed by the project team. This plan acts as the reference for the project and all partners will adhere to the Quality Assurance Plan.

Each project has its characteristics in terms of partners, work packages etc., and therefore requires a tailor-made Quality Assurance Plan, clear responsibilities and contact persons. The necessary information on the PRIViLEDGE project is described in Deliverable 6.1, "Project Reference Manual and Tools".

The quality management strategy of PRIViLEDGE is addressed in Section 2. It is divided in three key activities:

**Quality Planning:** Quality Planning comprises quality policies and procedures relevant to the project for both deliverables and processes, defines responsibilities and documents compliance. A corporate visual identity represents the project internally, in partner organisations, as well as externally. In order to communicate adequately within the project as well as to project external entities, several tools are established and explained in Section 2.1. Furthermore, project policies are described for document naming, for meetings or scientific publications, and so forth.

**Quality Assurance:** Quality assurance creates and monitors project processes that need to be performed effectively to reach the targeted outcome. This involves the establishment of interim reporting, clear responsibilities and regular, clearly guided meetings. These activities within PRIViLEDGE are summarised in Section 2.2.

**Quality Control:** Quality Control will be actively performed by all partners. A clear internal review process has been defined before deliverable submission to provide feedback to the editor. A proactive risk management has already been mentioned in the Description of Action. The risk management has been established as planned in order to guarantee the project quality and avoid delays or failures. Feedback on the project progress and outcomes by the Advisory Board will support the quality controlling and guide the project into the right direction. This is described in Section 2.3.

The target of the following section is to describe how all the mentioned pieces of the puzzle fit and stick together.

# 2 Quality Management Strategy

Quality is the degree to which the project fulfills its requirements. In order to fulfill and exceed the project requirements, a quality management strategy has been defined within the PRIViLEDGE project through three key processes, namely quality planning, quality assurance and quality control. These three processes are connected and interact in order to guarantee efficient and high-quality work.

## 2.1 Quality Planning

Quality planning determines quality policies and procedures relevant to the project for both deliverables and processes, defines who is responsible for what, and documents compliance.

### 2.1.1 Visual Identity

The creation of a common visual identity plays a significant role in the way the PRIViLEDGE project presents itself to both internal and external stakeholders. A corporate visual identity expresses the values and ambitions of our project and its characteristics. Our corporate visual identity makes the project visible and recognisable. It is of vital importance that people know of the existence of the project and remember its name and core mission at the right time. The following paragraphs present the actions that were taken in order to create a visual identity of the project.

**Logo.** For the improvement of its visibility, the PRIViLEDGE project has adopted a project logo. The logo is used on all internal templates as well as on external dissemination tools. This logo is depicted in Figure 1.



Figure 1: PRIViLEDGE project logo

**Templates.** Presenting the PRIViLEDGE project with a clear design is a claim by the whole consortium. Therefore, templates that bear the hallmark of the PRIViLEDGE design were created. All templates include the PRIViLEDGE logo, colours and the disclaimers.

To ease collaboration, LaTeX and MS Office (Formats: doc, ppt) templates were defined as the standard document format for all administrative and scientific documents. The templates are stored in the general project repository[1] in the `Templates` directory.

Templates for deliverables were designed to ensure not only a common visual standard for PRIViLEDGE documents, but also to find a general structure suitable for all deliverables. In the creation process it was taken into account that the partners include an executive summary, introduction, and a summary or conclusion into the document beside a clearly structured technical input.

---

[1]The repository can be found at `https://github.com/guardtime/priviledge-admin`.

**Leaflet.**  A leaflet for presenting the PRIViLEDGE project will be created as a part of Deliverable 5.2. An electronic version of the leaflet will also be made available on the PRIViLEDGE website.

**Project Website.**  The PRIViLEDGE project website is currently being developed, under the guidance of Guardtime but with feedback and input from all partners. It is expected to be available at the URL `https://www.priviledge-project.eu` by end of March 2018.

**Social Media.**  In order to reach a broad target group, Twitter and Facebook will be used as channels to raise awareness of project specific news, results and publications, and to foster cooperation activities. The accounts and sites will be created as part of Work Package 5 and reported in Deliverable 5.2.

### 2.1.2   Project Policies

Internal project guidelines, our so called project policies, were established to organise internal and external processes in terms of meetings, deliverables and publications, to ensure quality.

**Meetings.**  The consortium decided that the hosting partner of a meeting pays for conference facilities, catering and the like, while each partner pays for accommodation and provisions. Usually the host invites for lunch and coffee breaks during the meeting. Usually, each meeting will be accompanied by one common dinner. The meeting locations have to change regularly in order to achieve a fair distribution of costs. To keep costs down, we prefer to meet at company or academic facilities that can often be used for free. The following bullet points are supposed to work as a checklist for the host of upcoming meetings/workshops.

- We need one conference room for approximately 20-25 people. The room should be equipped with a projector as well as a flip chart or whiteboard, as well as power plugs for all participants.

- Are there any costs for the conference per room/day/person (e.g., coffee break, lunch)? Further expenses?

- Generally, Wifi connectivity should be provided for all participants.

**Deliverables.**  Deliverables are based on the templates that can be found in the `Templates` folder of the `priviledge-admin` git repository. Deliverables must be stored in the repository corresponding to the respective work package. The repositories can be accessed by all project participants under the following URLs:

**WP1:** `https://github.com/guardtime/priviledge-wp1`

**WP2:** `https://github.com/guardtime/priviledge-wp2`

**WP3:** `https://github.com/guardtime/priviledge-wp3`

**WP4:** `https://github.com/guardtime/priviledge-wp4`

**WP5, WP6, WP7:** `https://github.com/guardtime/priviledge-admin`

All scientific deliverables are written in LaTeX. Management deliverables may be written either in LaTeX or in Word. In either case, the directory shall contain a PDF file that is submitted to the EC for review.

The deliverables shall be stored in the repository corresponding to the work package, in a directory named `Dx.y Deliverable Title`, where `x.y` is the number of the deliverable and `Deliverable Title` is its title. Work documents are stored accordingly in folders named `Wx.y Work Document Title`. For work packages 5, 6, and 7, the document shall be stored in the directory `WP5 Communications`, `WP6 Project management`, or `WP7 Ethics`, respectively.

**Policy for publishing scientific papers.** Prior notice of any planned publication shall be given to the other parties concerned at least 30 days before the publication in accordance with the CA (8.4.2.1). Any objection to the planned publication shall be made in accordance with the GA in writing to the coordinator and to any party concerned within 30 days after receipt of the notice. If no objection is made within the time limit stated, the publication is permitted (CA 8.4.1). The beneficiaries may agree in writing on different time limits to those set above, which may include a deadline for determining the appropriate steps to be taken. Furthermore, the paper/article, or the link to it will be published on our official PRIViLEDGE project website. The coordinator (GT) shall be informed as soon as a link or document in PDF format is available. The Commission will then be informed about the scientific publication via our website and also via Twitter. All publications or any other dissemination relating to foreground that was generated with the assistance of financial support from the Union shall include the following statement (GA 29.4):

> This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 780477.

## 2.2 Quality Assurance

The focus of quality assurance is on the creation and monitoring of processes. Quality assurance creates and monitors project processes, which need to be performed effectively to reach the targeted outcome. This involves the establishment of interim reports, clear responsibilities and regular, clearly guided teleconferences.

### 2.2.1 Interim Reporting

The basic idea of interim reporting is to implement a tool that forces each partner to provide information regarding their ongoing and planned work as well as information on the resources spent. Two different levels of interim reporting are planned, on a three-month and on a half-year basis, as described in the CA (6.3.2.3.5) and the DoA (3.2.4). Additionally, and as described in Deliverable 6.1 "Project Reference Manual and Tools", extended reports are provided to the EC at M18 and M36. Report shall inform about:

- Main activities and main achievements since the last report.

- A summary of the resources (effort) consumed in each WP during the considered tranche.

All project partners are responsible:

- To provide the requested information completely, faithfully, and on time.

- To have close cooperation with the PC.

The PC will compile all inputs and generate reports per WP that will be verified with the WP leaders. This control action will help understand the project situation (by comparing with the work plans) and apply corrective measures when necessary. The information received within this internal reporting will be used by the PC as input for the production of a periodical report on the progress of the project to the entire consortium.

The generation of the reports needs collaboration from all project partners and is organised as follows.

**Three-monthly reports:** Each WP leader will write and send an internal management report to the PC, by collecting contribution from partners in the WP using the template provided by the project. The report shall describe the technical and management work done; it will report difficulties, achieved milestones and deliverables, patents, publications, travel and relevant events.

**Six-monthly reports:** Each partner submits a report detailing progress and effort expenditure, using the template provided by the project. These reports are collected by the PC. Each WP leader will in addition answer a questionnaire, structured in three major sections: (1) assessment of the work done vs. the planned

work; (2) key issues for the development of PRIViLEDGE; (3) on-going results of evaluation indicators. Based on these individual questionnaires, Guardtime as WP6 leader will analyse all the self-assessment questionnaires and summarise the overall project progress, to be presented as reports to the PMC for further analysis and actions as necessary.

**Reports at M18 and M36:** Each partner prepares a financial statement, which is collected and presented to the EC by Guardtime. The partner reports mentioned in previous point are used to generate the annual project management report to the EC and to be presented also in the General Assembly of PRIViLEDGE.

### 2.2.2 Responsibilities and Internal Review

Transparency of roles and responsibilities has a big impact on the project success. Uncertainty can dramatically affect individual, organisational as well as consortium performance. Therefore, in Deliverable 6.1, responsible persons for each organisation and per WP were defined. In a further step responsibilities for deliverables were defined. Tables 1 and 2 list all deliverables due within the first and last 18 months of the project, respectively. While deliverable-leading organisations were already defined within the DoA, the concrete editor responsible for requesting and guiding partner inputs towards a punctual and high-quality submission, are appointed only during the project. In line with the concluded internal review process (described in Section 2.3.2) two internal reviewers for each deliverable were defined and clear deadlines for first draft version, the review feedback as well as for the submission were established. The reviewers for each document are assigned at the physical PMC/TMC meeting that precedes the completion of the respective deliverable.

### 2.2.3 Teleconferences and Meetings

Communication is one of the most essential foundations of successful project collaborations. Therefore, the PRIViLEDGE consortium established regular teleconferences or online meetings, which will usually employ the Zoom online meeting service on Guardtime's account. These virtual meetings are planned in addition to face-to-face meetings.

In between the virtual or face-to-face meetings, close collaboration of the project partners is achieved by means of a mailing list (`priviledge@guardtime.com`) as well as a joint workspace at the Slack online collaboration service, which provides instant person-to-person and group communication. Slack channels exist, amongst others, for the technical work packages as well as for broader topics such as project administration or communication.

To ensure the project success, it is necessary to implement an efficient meeting structure. At the onset of the PRIViLEDGE project, the kick-off meeting took place together with the first GA meeting from January 15–17, 2018, at the IBM Research site in Rüschlikon, Switzerland. The different partners' expectations and schedules were discussed in order to make a definitive plan about the further work plan and required actions. We then went on to establish a monthly PMC/TMC teleconference during which the status of each WP is reported and discussed, along with general matters concerning the project organization. We plan two face-to-face PMC/TMC meetings per year, co-located with the GA meetings.

For the technical work packages, we have set up regular monthly online meetings to discuss the project advances among all work package participants. We will set up additional calls between partners collaborating on specific technical topics on demand. In addition, we intend to organize several WP-internal/cross-WP face-to-face workshops whenever necessary. Intensive two-day face-to-face workshops can provide a deeper exchange than what can be achieved by an online meeting.

At the end of each project period there will be a review preparation meeting one day before the official review meeting takes place (planned venue: EC premises in Brussels, or if applicable partner's premises).

Furthermore PRIViLEDGE will organize and participate in workshops, conferences, and other events as described in the Grant Agreement.

---

[2]This task was initially assigned to Zenith Analytics, and is temporarily re-assigned to University of Edinburgh.

| Num | Deliverable title | Partner | Editor | WP | Month | Draft due | Review due | Reviewers |
|---|---|---|---|---|---|---|---|---|
| D6.1 | Project Reference Manual and Tools | GT | Mirjam Kert | WP6 | M3 | 28.02.2018 | 09.03.2018 | UEDIN[2], IBM |
| D6.2 | Quality Assurance Plan | IBM | Björn Tackmann | WP6 | M3 | 28.02.2018 | 09.03.2018 | GRNET, GT |
| D2.1 | State of the art on Privacy-Enhancing Cryptography for Ledgers | UT | Helger Lipmaa | WP2 | M6 | 31.05.2018 | 08.06.2018 | GT, TUE |
| D5.1 | Initial Communication and Dissemination Plan | GT | Mirjam Kert | WP5 | M6 | 31.05.2018 | 08.06.2018 | UNISA, IBM |
| D7.1 | Ethics requirements | GT | Mirjam Kert | WP7 | M6 | 31.05.2018 | 08.06.2018 | |
| D3.1 | State of the Art of Cryptographic Ledgers | UEDIN | Aggelos Kiayias | WP3 | M8 | 31.07.2018 | 10.08.2018 | UNISA, UEDIN[2] |
| D5.2 | Communication and Dissemination Toolkit | GT | Mirjam Kert | WP5 | M8 | 31.07.2018 | 10.08.2018 | |
| D5.3 | Exploitation Strategy and Roadmap | IBM | Björn Tackmann | WP5 | M9 | 31.08.2018 | 07.09.2018 | |
| D1.1 | Requirements and Interface Design | GRNET | Panos Louridas | WP1 | M12 | 30.11.2018 | 07.12.2018 | |
| D5.4 | Updated Consolidated Communication and Dissemination Plan | GT | Mirjam Kert | WP5 | M12 | 30.11.2018 | 07.12.2018 | |
| D2.2 | Definitions and Notions of Privacy-Enhancing Cryptographic Primitives for Ledgers | UNISA | Ivan Visconti | WP2 | M18 | 31.05.2019 | 07.06.2019 | |
| D4.1 | Report on Architecture of Secure Ledger Systems | UEDIN | Aggelos Kiayias | WP4 | M18 | 31.05.2019 | 07.06.2019 | |
| D6.3 | First Scientific & Research Impact Measurement | IBM | Christian Cachin | WP6 | M18 | 31.05.2019 | 07.06.2019 | |

Table 1: Deliverables during the first reporting period

## 2.3 Quality Control

The focus of quality control is on feedback and deviation management in the project. Quality control ensures that feedback, from internal as well as from external advisors, is taken into account and therefore positively influences the work towards project objectives. Risk Management forms a central focus of quality control as the proactive notice of deviations allows the consortium to control the consequences or even transform them and profit from positive effects.

### 2.3.1 Advisory Board

The consortium will be supported and advised by an external Advisory Board (AB), consisting of four selected persons from European organisations not directly involved in the project as partners. The AB members will provide an external unprejudiced view advising on strategic directions of the project in terms of detailed technical goals and impact, comment on economical feasibility and achieved or missed targets. They will be involved as project internal reviewers, as well as ambassadors and promoters, by suggesting synergies with their own

| Num | Deliverable title | Partner | Editor | WP | Month | Draft due | Review due | Reviewers |
|---|---|---|---|---|---|---|---|---|
| D3.2 | Design of Extended Core Protocols | TUE | Berry Schoenmakers | WP3 | M24 | 30.11.2019 | 06.12.2019 | |
| D4.2 | Report on Architecture for Privacy-Preserving Applications on Ledgers | GRNET | Panos Louridas | WP4 | M24 | 30.11.2019 | 06.12.2019 | |
| D1.2 | Validation Criteria | UEDIN[2] | | WP1 | M30 | 31.05.2020 | 09.06.2020 | |
| D2.3 | Improved Constructions of Privacy-Enhancing Cryptographic Primitives for Ledgers | UNISA | Ivan Visconti | WP2 | M30 | 31.05.2020 | 09.06.2020 | |
| D4.3 | Final Report on Architecture | IBM | Björn Tackmann | WP4 | M30 | 31.05.2020 | 09.06.2020 | |
| D5.5 | Report on Exploitation | IBM | Björn Tackmann | WP5 | M33 | 30.08.2020 | 09.06.2020 | |
| D1.3 | Use Case Validation | SCCEIV | Sven Heiberg | WP1 | M36 | 30.11.2020 | 08.12.2020 | |
| D2.4 | Revision of Privacy-Enhancing Cryptographic Primitives for Ledgers | UT | Helger Lipmaa | WP2 | M36 | 30.11.2020 | 08.12.2020 | |
| D3.3 | Revision of Extended Core Protocols | UEDIN | Aggelos Kiayias | WP3 | M36 | 30.11.2020 | 08.12.2020 | |
| D4.4 | Report on Tools for Secure Ledger Systems | IBM | Björn Tackmann | WP4 | M36 | 30.11.2020 | 08.12.2020 | |
| D4.5 | Report on Tools for Privacy-Preserving Applications on Ledgers | GT | Ahto Truu | WP4 | M36 | 30.11.2020 | 08.12.2020 | |
| D6.4 | Second Scientific & Research Impact Measurement | IBM | Christian Cachin | WP6 | M36 | 30.11.2020 | 08.12.2020 | |

Table 2: Deliverables during the second reporting period

activities and activities of their networks and bodies, and by keeping their networks informed of the project activities and outcomes, thus supporting wider visibility and promoting the project cooperation in the ICT area. They also actively contribute to the project by notifying the project team on the latest scientific and technological evolutions in the ICT area, new initiatives, and so forth.

Through the integration of an Advisory Board, interim feedback of enormous importance regarding the overall orientation of the project outcome is expected. This supports the path towards objectives and controls the quality of the project work as well as the quality of expected outcomes.

### 2.3.2 Internal Review Process

To ensure quality of Deliverables, an internal review process has been defined. The main goal of this process is to establish internal feedback by partners who did not directly participate as editor to the Deliverable before submitting the Deliverable to the European Commission. The review process is shown in Figure 2 and explained below.

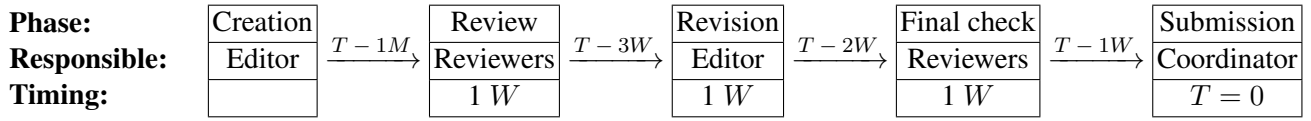| Phase: | Creation | | Review | | Revision | | Final check | | Submission |
|---|---|---|---|---|---|---|---|---|---|
| **Responsible:** | Editor | $\xrightarrow{T-1M}$ | Reviewers | $\xrightarrow{T-3W}$ | Editor | $\xrightarrow{T-2W}$ | Reviewers | $\xrightarrow{T-1W}$ | Coordinator |
| **Timing:** | | | $1\,W$ | | $1\,W$ | | $1\,W$ | | $T=0$ |

Figure 2: Depiction of the review process of project deliverables. The times on arrows denote the due dates for the completion of the preceding action, relative to the submission time $T$, in weeks ($W$) or months ($M$).

**Phase 1: Creation.** Document editor collaborates with all relevant partners in the respective work package to produce the document. The document is written in LaTeX or, if it is a deliverable in WP5–WP7, alternatively in Word. The document is stored in the respective git repository and sent to the reviewers one month prior to the submission date.

**Phase 2: Review.** Reviewers read the draft and compare the content against its objective as defined in the work draft. For LaTeX deliverables, obvious typos can be corrected directly in the source files. Comments shall be written either using an appropriate LaTeX package (e.g., `comments.sty`), or by annotating the PDF file. For Word deliverables, obvious typos can be corrected with change tracking enabled. Other comments shall be added as "Word comments".

**Phase 3: Revision.** The document editor and the relevant partners address the review comments, and send the document for a final check to the reviewers.

**Phase 4: Final check.** The reviewers check whether their comments have been properly addressed. Potentially remaining open issues are resolved in direct communication between the reviewers and the responsible partners. After the final check, the reviewers notify the Coordinator.

**Phase 5: Submission.** The Project Coordinator uploads the completed files to the EU portal.

### 2.3.3 Internal Work Documents

To further ensure proper advancement in the project, certain deliverables that are key to the progress of other parts of the project are preceded by internal work documents that allow to check whether the expected result matches the requirements of other parts of the project. The work documents are listed in Table 3. Just like deliverables, internal work documents also have to pass a project-internal review process. This process, however, is simpler than the one for regular deliverables and is depicted in Figure 3.

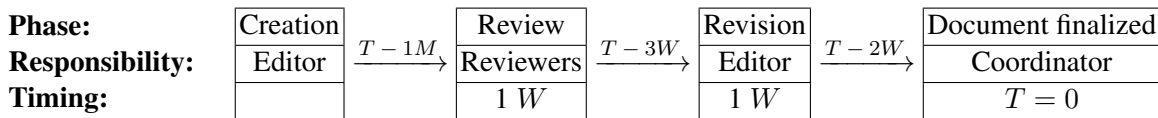| **Phase:** | Creation | | Review | | Revision | | Document finalized |
|---|---|---|---|---|---|---|---|
| **Responsibility:** | Editor | $\xrightarrow{T-1M}$ | Reviewers | $\xrightarrow{T-3W}$ | Editor | $\xrightarrow{T-2W}$ | Coordinator |
| **Timing:** | | | $1\,W$ | | $1\,W$ | | $T=0$ |

Figure 3: Depiction of the review process of work documents. The times on arrows denote the due dates for the completion of the preceding action, relative to the finalization time $T$, in weeks ($W$) or months ($M$).

### 2.3.4 Risk Management

To guarantee the achievement of the objectives of the PRIViLEDGE project, it is essential to identify and understand the significant project risks.

The continuous risk management process is based on the early identification of, and the fast reaction to, events that can negatively affect the outcome of the project. The frequent meetings of the project bodies therefore serve

as the main forum for risk identification. The identified risks are then analysed and graded, based on impact and probability of occurrence.

Technical risks were analysed and graded, based on their probability of occurrence in order to answer the governing question: "How big is the risk, and what is its potential impact?" Knowing how a risk impacts the project is important as several risks of the same type can be an indication of a larger problem. The following table shows the initial risk assessment for the PRIViLEDGE project.

| Description of risk | WPs | Countermeasures |
|---|---|---|
| A partner withdraws or is unable to provide a foreseen contribution<br><br>Probability: Low<br>Severity: High<br>Overall Level: Low | All WPs in which that partner is involved | A strong and thorough Consortium Agreement before the Grant Agreement ensures keeping original commitments on track and managing such unlikely situation professionally. The team composition of the consortium ensures a balance of skills. The very experienced Project Management team is committed to monitoring the progress of each partner and promptly reacting where required. In the unlikely case of all measures failing, the consortium will consider bringing a new partner into the consortium, upon consultation with the EU Project Officer. The consortium members have a deep knowledge of the stakeholders in the field, and can easily find a replacing partner. |
| Lack of coherence in project work flow and lack of cooperation among partners.<br><br>Probability: Minimal<br>Severity: Very high<br>Overall Level: Low | All WPs | Most consortium members are very familiar and experienced in working with one another due to previous work together. In addition, the tight monitoring of each partner's progress by the strong project management team will ensure coherence in the overall project. |
| Budget overspending.<br><br>Probability: Low<br>Severity: Medium<br>Overall Level: Low | All WPs | The project coordinator will be informed in advance of WP leaders' intentions for meeting and travel, as well as for equipment spending, so as to make full use of synergies. Regular review of is foreseen by the management of this project. Budget has been calculated well from the beginning to avoid any risk to overspending. |
| Critical deliverables are delivered too late and milestones are missed.<br><br>Probability: Low<br>Severity: High<br>Overall Level: Low | All WPs | WP6 has envisioned specific processes on how to coordinate and manage the project in an efficient way. Planning the progress of work with internal deadlines well in advance and at the beginning of the project will deliver successful delivery of results on time. Partners that have delays in their tasks will allocate additional resources to meet the planned deadlines. Important deliverables are preceded by "first versions" of the work, so problems can be identified and addressed early. The reviewing process for deliverables also ensures close monitoring. |
| Issues regarding IPR.<br><br>Probability: Low<br>Severity: High<br>Overall Level: Low | All WPs | A Consortium agreement will have specific provisions on resolving IPR issues. |

| Failure to exploit and market project results.<br><br>Probability: Low<br>Severity: High<br>Overall Level: Low | WP6 | The PRIViLEDGE consortium includes partners with excellent expertise in their market sectors and related dissemination possibilities. Each partner has already a clear idea of their exploitation needs at the beginning of the project. |
|---|---|---|
| Inadequate involvement of policy makers.<br><br>Probability: Low<br>Severity: High<br>Overall Level: Low | WP5 | The PRIViLEDGE consortium is already very much involved in different policy initiatives on the European level such as the Cybersecurity Public-Private Partnership that was set up by the European Commission and the European Industry jointly to further the European industrial initiatives. |
| Platform Dependence in UC4.<br><br>Probability: Low<br>Severity: Medium<br>Overall level: Low | WP1 & WP4 | For the Software Update System to be useful and robust, it will have to be platform independent. This, however, poses a risk: Each of the major platforms (Windows, Linux, Apple) comes in various different versions. To make matters worse, each single machine will have its individual configuration. The Software Update System should be able to handle all those platforms, versions and configurations reliably. To mitigate this risk, there are at least the following two options: (a) exhaustive tests (on as many platforms and versions as possible), (b) a definitive list of supported platforms, versions and required configurations. |
| Failure to assess potential nonalignment between the requirements defined in WP1 and the approaches and prototypes that will be developed.<br><br>Probability: Low<br>Severity: Medium<br>Overall Level: Low | WP1 | To address this challenge, a continuous assessment will take place to make sure that the approaches and protocols developed in WP2 and WP3, and the prototypes and toolkits developed in WP4 will meet the requirements of each use case. These checks will occur iteratively until the end of the project and will be documented in two working documents. In addition, the partners providing technology will work closely with partners responsible for the use cases. In turn, use case partners will provide feedback to the partners involved in the implementation of the prototypes. |
| Use cases require some new privacy-enhancing cryptographic primitives but PRIViLEDGE proves that constructing them with standard security guarantees is impossible.<br><br>Probability: Medium<br>Severity: Low<br>Overall level: Low | WP2 | The "provable security" approach used to prove the security of candidate constructions of cryptographic primitives sometimes also shows impossibility results (i.e., there exists no construction of a cryptographic primitive that can be as privacy-enhancing as desired by some applications). While the above risk is certainly concrete, there exist several approaches to circumvent an impossibility result, therefore providing an alternative security guarantee that is usually sufficient for the applications. PRIViLEDGE is aware that along the way some impossibility results could be demonstrated, and will use various heuristics (e.g., the RO model, knowledge and timing assumptions) that have already been used in the past as concrete alternative paths that bypass the impossibility barrier. |

| Limited scalability of developed cryptographic protocols.<br><br>Probability: Low<br>Severity: Medium<br>Overall level: Low | WP3 | Cryptographic protocols are designed to withstand the strongest type of attacks and adversaries. However, high security levels may incur considerable performance costs, and may thus become impractical for some of the use-cases targeted by the project, e.g., when processing huge volumes of data. PRIViLEDGE aims to resolve such a performance problem by reverting to a weaker adversarial model, e.g., by assuming passive adversaries rather than active adversaries. |
|---|---|---|
| Implementations of developed techniques are not sufficiently efficient/scalable.<br><br>Probability: Low<br>Severity: High<br>Overall level: Low | WP4 | Newly developed cryptographic schemes and protocols may face the issue of not being sufficiently efficient or scalable for practical applications. The PRIViLEDGE consortium is aware of this risk, and includes partners that have a proven track record in improving the efficiency of cryptographic schemes (e.g. for NIZKs and SNARKs), as well as partners that are experienced in implementing cryptographic techniques. Furthermore, the project will ensure close collaboration between the partners to ensure quick feedback on where efficiency improvements are needed. |

The risks will be further monitored on a quarterly basis and an updated risk table will be provided within the Periodic Reports.

Notably, the first risk described in the table did already materialize, as one partner named in the project proposal (Zenith Analytics) will not be able to fulfill their role. The remaining PRIViLEDGE project partners are committed to solving this scenario by including a proficient industry partner that can take over the tasks originally assigned to Zenith Analytics.

| Num | Deliverable title | Partner | Editor | WP | Month | Draft due | Review due | Reviewers |
|---|---|---|---|---|---|---|---|---|
| W1.0 | Requirements from use cases | GRNET | Panos Louridas | WP1 | M3 | 31.03.2018 | 06.04.2018 | UT, TUE |
| W2.1 | First Report on Existing Privacy-Enhancing Cryptographic Primitives for Ledgers | UT | Helger Lipmaa | WP2 | M4 | 30.04.2018 | 07.05.2018 | UEDIN, GUNET |
| W3.1 | First Report on State of the Art of Cryptographic Ledgers | TUE | Berry Schoenmakers | WP3 | M5 | 31.05.2018 | 07.06.2018 | IBM, SC-CEIV |
| W2.2 | First Report on Definitions and Notions of Privacy-Enhancing Cryptographic Primitives for Ledgers | UNISA | Ivan Visconti | WP2 | M12 | 31.12.2018 | 08.01.2019 | |
| W1.1 | Work Package Alignment: First Report | GRNET | Panos Louridas | WP1 | M15 | 31.03.2019 | 05.04.2019 | |
| W4.1 | First Report on Architecture of Secure Ledger Systems | UEDIN | Aggelos Kiayias | WP4 | M15 | 31.03.2019 | 05.04.2019 | |
| W3.2 | First Report on Design of Extended Core Protocols | UEDIN | Aggelos Kiayias | WP3 | M18 | 30.06.2019 | 05.07.2019 | |
| W4.2 | First Report on Architecture for Privacy-Preserving Applications on Ledgers | GRNET | Panos Louridas | WP4 | M21 | 30.09.2019 | 07.10.2019 | |
| W1.2 | Work Package Alignment: Second Report | GT | Ahto Truu | WP1 | M24 | 31.12.2019 | 07.01.2020 | |
| W2.3 | First Report on Improved Constructions of Privacy-Enhancing Cryptographic Primitives for Ledgers | UNISA | Ivan Visconti | WP2 | M24 | 31.12.2019 | 08.01.2020 | |

Table 3: Deliverables during the second reporting period

# 3   Summary

This Quality Assurance Plan demonstrates that quality aspects are taken into account in a variety of processes and activities within the PRIViLEDGE project. The interrelated quality processes—planning, assurance and control—impact the project work from its start to its end. The project aims at obtaining a high degree of quality, where outcomes are achieved in terms of the effectivity and efficiency of working practices, as well as products, and standards of project deliverables and outputs. This plan seeks to establish the procedures and standards to be employed in the project, and to allocate responsibility for ensuring that these procedures and standards are followed. The plan is effective throughout the lifetime of the project, but is open to revision if necessary. Responsibilities for quality planning, assurance and control are shared between all partners, which allow various views on quality issues in order to reach the optimal outcome.