

PROJECT PROMETHEUS
PRivacy preserving pOst-quantuM systEms
from advanced crypTograpHic mEchanisms
Using latticeS



D1.1

Project quality plan

Contractual submission date
Month 6


Deliverable version
1.0

Actual submission date
June 2019

Main author
Laurent Grémy, Quentin Toutou (ENSL)



<http://www.h2020prometheus.eu/>

 h2020prometheus

PROMETHEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701. The contents of this deliverable are the responsibility of the PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.

Document information

| | |
|-----------------------|---|
| Grant agreement no. | 780701 |
| Project acronym | PROMETHEUS |
| Project full title | PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS |
| Type of action | Research and Innovation Action (RIA) |
| Topic | H2020-DS-06-2017-Cybersecurity PPP: Cryptography |
| Project dates | 1 st January 2018 (Month 1) / 31 st December 2021 (Month 48) |
| Duration | 48 months |
| Project URL | http://www.h2020prometheus.eu/ |
| EU Project Officer | Carmen IFRIM |
| Work package | WP1 – Management and coordination |
| Deliverable title | Project quality plan |
| Deliverable no. | D1.1 |
| Deliverable version | 1.0 |
| Deliverable filename | PROMETHEUS-WP1-D1.1.pdf |
| Nature of deliverable | Report |
| Dissemination level | Public |
| Number of pages | 32 |
| Responsible partner | ENSL (participant number 1) |
| Author | Laurent Grémy, Quentin Touitou (ENSL) |

Abstract. The main aim of the Project handbook is at first to generate a document that will explain the numerous procedures and tools that will be used by the PROMETHEUS consortium to ensure efficient implementation of the work plan. It then provides a reference guide for the management procedures and protocols used within the project. Finally, it shows how we plan to ensure the project progresses in accordance with the agreed objectives. Each project participant can use the handbook to find information on the project management rules that the PROMETHEUS consortium will use in order to maintain a high level of project quality. The control of the correct execution of the procedures defined in this Project handbook will be a responsibility of the Project Coordinator who is mainly responsible for project management and project execution related activities.

Keywords: Dissemination, communication.

Signatures

| | | | |
|-------------|---|------|------------|
| Written by | Laurent Grémy, Quentin Toutou | ENSL | 12/2018 |
| Reviewed by | Emilie Sablon | ENSL | 10/05/2019 |
| Reviewed by | Octavie Paris | ENSL | 03/06/2019 |
| Approved by | Benoît Libert as Project coordinator | ENSL | 12/05/2019 |
| Approved by | Sébastien Canard as Technical leader | ORA | 12/05/2019 |

Partners

| | |
|--------------|---|
| ENSL | ENS de Lyon |
| ORA | Orange SA |
| CWI | Centrum voor Wiskunde en Informatica |
| IDC | Interdisciplinary Center Herzliya |
| RHUL | Royal Holloway, University of London |
| RUB | Ruhr-Universität Bochum |
| SCYTL | Scytl Secure Electronic Voting, S.A. |
| THA | Thales Communications & Security S.A.S. |
| TNO | Nederlandse organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek |
| UPC | Universitat Politècnica de Catalunya · BarcelonaTech |
| UR1 | Université de Rennes 1 |
| WEI | Weizmann Institute of Science |

Acronyms

| | |
|--------------|--|
| DM | Dissemination Manager |
| DoA | Description of the Action |
| EB | Executive Board |
| EC | European Commission |
| EM | Exploitation Manager |
| EU | European Union |
| GA | Grant Agreement |
| GEOM | Gender and Equal Opportunity Manager |
| INRIA | Institut national de recherche en informatique et en automatique |
| IPR | Intellectual Property Rights |
| PC | Project Coordinator |
| PDF | Portable Document Format |
| QM | Quality Manager |
| SAB | Scientific Advisory Board |
| TL | Technical Leader |
| WP | Work Package |

Contents

| | | |
|----------|---------------------------------------|-----------|
| 1 | Project information | 5 |
| 2 | Legal Aspects | 6 |
| 2.1 | Grant Agreement | 6 |
| 2.2 | Consortium Agreement | 7 |
| 2.3 | Amendments | 7 |
| 2.4 | Payment | 9 |
| 3 | Project structure | 9 |
| 3.1 | Work packages and tasks | 9 |
| 3.2 | Partners | 12 |
| 3.3 | Team management | 14 |
| 3.4 | Making decision | 17 |
| 4 | Quality processes | 19 |
| 4.1 | Visual identity | 19 |
| 4.2 | Communication | 19 |
| 4.3 | Publications | 21 |
| 4.4 | Deliverables and milestones | 22 |
| 4.5 | Meetings | 24 |
| 5 | Quality assurances | 27 |
| 5.1 | Management reports | 27 |
| 5.2 | Review workflow | 29 |
| 5.3 | Risk management | 30 |
| 6 | Conclusion | 32 |

1 Project information

The PROMETHEUS project aims to provide post-quantum signature schemes, encryption schemes and privacy-preserving protocols relying on lattice. In order to reach the goals of the project, the PROMETHEUS consortium has adopted an organization to maximise the efficiency of PROMETHEUS. This document will describe the structure of the project, the quality processes we adopt and the way to ensure this quality.

The general project information are given in Table 1 and the list of beneficiaries is described in Table 2.

| | |
|------------------------|---|
| Project title | PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using lattices |
| Project Number | 780701 |
| Starting date | 01/01/2018 |
| Duration | 48 months |
| Project Officer | Carmen IFRIM |
| Call (part) identifier | H2020-DS-LEIT-2017 |
| Topic | H2020- DS-06-2017- Cybersecurity PPP: Cryptography |
| Website | http://www.h2020prometheus.eu/ |

Table 1: General project information

| N° | Participant organisation name | Short name | Country |
|-----|---|------------|----------------|
| P1 | ECOLE NORMALE SUPERIEURE DE LYON | ENSL | France |
| P2 | ORANGE SA | ORA | France |
| P3 | TICHTING CENTRUM VOOR WISKUNDE EN INFORMATICA | CWI | Netherlands |
| P5 | ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE | RHUL | United Kingdom |
| P6 | RUHR-UNIVERSITAET BOCHUM | RUB | Germany |
| P7 | SCYTL SECURE ELECTRONIC VOTING SA | SCYTL | Spain |
| P8 | THALES COMMUNICATIONS AND SECURITY SAS | THA | France |
| P9 | NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK | TNO | Netherlands |
| P10 | UNIVERSITAT POLITECNICA DE CATALUNYA | UPC | Spain |
| P11 | UNIVERSITE DE RENNES I | UR1 | France |
| P12 | WEIZMANN INSTITUTE OF SCIENCE | WEI | Israel |
| P13 | INTERDISCIPLINARY CENTER HERZLIYA | IDC | Israel |

Table 2: List of beneficiaries

The main contact points are the followings.

- Coordinator: Dr. Benoît LIBERT (benoit.libert@ens-lyon.fr, +33 4 26 23 39 32).
- Technical leader: Dr. Sébastien CANARD (sebastien.canard@orange.com, +33 2 31 15 91 88).
- Coordinator's research contract administration: ingenierie.projets@ens-lyon.fr.

2 Legal Aspects

The project operates within the Horizon 2020 Framework Programme. This Project Management Guide relates to Grant Agreement N°. 780701. A Consortium Agreement has been signed by all the beneficiaries. For the avoidance of doubt, the Grant Agreement and Consortium Agreement take precedence over this document. The Grant Agreement takes priority in all circumstances.

2.1 Grant Agreement

2.1.1 The grant agreement N°780701

The Grant Agreement forms the legal basis for the implementation of the project. It consists of:

- Terms and Conditions (this is the core contract);
- Annex 1 Description of the action (DoA);
- Annex 2 Estimated budget for the action;
- Annex 3 Accession Forms;
- Annex 4 Model for the financial statements;
- Annex 5 Model for the certificate on the financial statements;
- Annex 6 Model for the certificate on the methodology.

Although the core contract is signed between the EU and the Coordinator of the project, all partners have become individual contract partners with the commission by signing the Accession Forms. The Grant Agreement must be kept by all partners and should be provided to the auditor in case of an audit.

2.1.2 The amendment N°AMD-780701-7

The amendment AMD-780701-7 provides an update of the consortium, the budget and the Description of the Action. It consists of :

- Amendment terms and conditions;
- Annex 1 Description of the action (DoA);
- Annex 2 Estimated budget for the action.

2.2 Consortium Agreement

Whereas the Grant Agreement is signed between the EU and the partners, the Consortium Agreement is signed between the partners themselves. It arranges in more detail the provisions of the Grant Agreement, such as but not limited to: financial issues, payments, management, decision making, conflict resolution, intellectual property rights and liability. The Consortium Agreement must also be kept by the partners and must be shown in case of audits.

2.3 Amendments

2.3.1 Definition

An amendment to the Grant Agreement is a legal act modifying the commitments initially accepted by the parties and which may create new rights or impose new obligations on them, or modifying significant parts of the Grant Agreement. It allows the parties to modify the GA during its lifetime.

2.3.2 Cases when the GA must be amended

- Changes involving beneficiaries & linked third parties
 - Adding a new beneficiary
 - Deletion of a beneficiary whose participation has been terminated because:
 - * it has not signed the grant agreement
 - * it has not provided a declaration on joint & several liability as requested
 - * for some other reason
 - Change of beneficiary due to 'partial takeover'
 - Deletion or addition of linked third party (Article 14)
 - Specific case: if a beneficiary's participation is terminated at the initiative of other beneficiaries (Article 50.2)
- Change involving the coordinator/principal beneficiary
 - Change of coordinator
 - Change in the bank account the coordinator uses for payments
 - Change in the 'authorisation to administer' option
- Changes affecting the project or its implementation
 - Change to Annex 1
 - Change in the title of the project or its acronym, starting date, duration or reporting periods
 - Resumption of project activities after a temporary suspension
- Changes involving the financial aspects of the grant
 - Change to Annex 2 or 2a

- Change in the maximum grant amount, reimbursement rate(s), the estimated eligible costs of the project, the amount of pre-financing or the contribution to the Guarantee Fund
- Change concerning specific cost categories ('specific unit costs')

2.3.3 Cases when amendments are NOT necessary

- for certain budget transfers;
- if the name or address of a beneficiary, linked third party or coordinator changes;
- if a universal takeover results in a change of beneficiary;
- if there is a change in the name of the bank or the address of the branch where the coordinator has an account, or in the name of the account holder.

2.3.4 Who can request an amendment?

The consortium is free to propose amendments. The coordinator will have to check that the consortium has reached agreement through an internal decision-making process, as set out in the Consortium Agreement (e.g. unanimously or by simple or qualified majority) prior to its submission to the European Commission.

Exception: in cases where coordinators are to be replaced without their agreement, another beneficiary (acting on behalf of the other beneficiaries in the consortium) submits the request. NB: The European Commission can also propose amendments.

2.3.5 Request for an amendment

This comprises 2 documents generated automatically by the coordinator from the project EU portal:

1. the letter requesting an amendment
2. the amendment

Once the request for an amendment is complete and ready to be submitted, the system generates the 2 documents and prompts the coordinator to e-sign. Before submission, at any time during preparation, the draft versions are available for preview as a PDF file under the 'Documents' tab.

- The letter requesting an amendment provides justification for the request, using material from the 'justification' field in the 'amendment information' tab. The request is assessed on the basis of whatever information and explanations the coordinator provides.
- Annexes & supporting documents: the user is always prompted to upload any documents to be included with the request for an amendment. These depend on the type of amendment and the specific case.
 - Some supporting documents may be mandatory (e.g. to add a new beneficiary, the new beneficiary must e-sign the 'Declaration of Honour' and the 'Accession Form' (Annex 3 to the Model Grant Agreement).

- It will be decided on a case-by-case basis whether other supporting documents/annexes are needed.

The amendment is the legal document containing the amendments to the Grant Agreement. It is legally binding and will be incorporated into the agreement. Once the request for an amendment is complete and ready for submission, the amendment request letter and the amendment are automatically generated. The Commission can accept or reject the request within 45 days. It sends the coordinator a formal notification through the Participant Portal. If no notification is received within the 45-day deadline, the request is considered to have been rejected (tacit rejection). The details of the amendment procedure are available in the EC portal.

2.4 Payment

The following types of payments are foreseen:

- Pre-financing payment at the beginning of the project: Pre-financing funds remain EU property until they are ‘cleared’ against eligible costs accepted by the European Commission.
- Interim payments based on submitted and accepted costs by the EC
 - Retention until final payment (10%) + Guarantee Fund (5%)
 - Last interim payment by the EC within the 85% limit of the maximum contribution
 - Released after the approval of the periodic reports
- Final payment following the approval of the final report: it will be transferred after the approval of the final report and consists of the difference between the calculated EU contribution (on the basis of the eligible costs) minus the amounts already paid.

3 Project structure

We then give some details about the project structure, describing the work packages, partners and the way the consortium is working to exchange and make decision.

3.1 Work packages and tasks

3.1.1 Work packages

The low level implementation of the organization of PROMETHEUS is the Work Packages (WPs). The target of this structure, underlying the work plan, is to meet the project’s main concepts and objectives. PROMETHEUS is split into seven WPs, with significant dependencies and expected synergies among them. The WPs are further structured in tasks. The interdependencies between the WPs are given in Figure 1.

- WP1 “Management and Coordination” draws from the input of all other WPs to ensure a successful project lifetime with respect to risk and innovation.

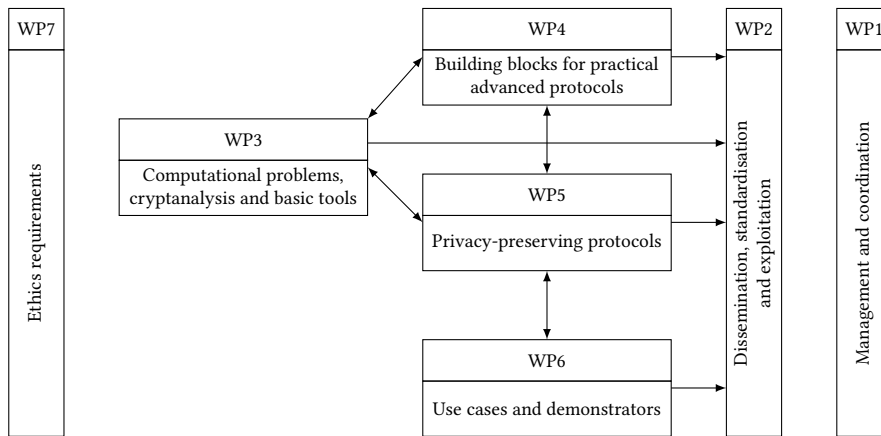


Figure 1: WP interdependency chart.

- WP2 “Dissemination, standardisation and exploitation” obtains inputs from technical and scientific WPs and ensures the communication and dissemination of their results to outside parties as well as to participating entities.
- WP3 “Computational problems, cryptanalysis and basic tools” poses the foundations of lattice-based cryptography, in order to drive the design of cryptographic schemes in WP4-5.
- WP4 “Building blocks for practical advanced protocols” designs and implements lattice-based cryptographic building blocks. This will serve as a basis for the implementation of WP5 and WP6.
- WP5 “Privacy-preserving protocols” designs and implements specific cryptographic protocols for the protection of individuals’ privacy. The proposed protocols will be based on lattices, taking as building blocks the results of WP4 and the security hypotheses of WP3. This will be a strong basis for use case demonstrators performed in WP6.
- WP6 “Use cases and demonstrators” builds e-voting, e-consumer, anonymous credentials and cyber threat intelligence systems using the results of the technical WP3, WP4 and WP5.
- WP7 “Ethics requirements” ensures compliance with the ethics requirements set out in WP 1.

3.1.2 Tasks

The different purposes of a WP are divided into tasks, which ensure the coherence of the different related deliverables of the WP. Table 3 references the different tasks.

| No. | Title | Lead beneficiary | Start date | End date |
|--|---|------------------|------------|----------|
| Work package 1: management and coordination | | | | |
| 1 | Administrative and resources management | ENSL | 1 | 48 |
| 2 | Scientific and technical management | ORA | 1 | 48 |
| 3 | Risk management | ENSL | 1 | 48 |
| 4 | Legal and ethical framework | ENSL | 1 | 48 |
| Work package 2: dissemination, standardisation and exploitation | | | | |
| 1 | Exploitation and innovation management | ORA | 1 | 48 |
| 2 | Dissemination planning and activities | ENSL | 1 | 48 |
| 3 | Standardisation and NIST process | RHUL | 1 | 48 |
| Work package 3: computational problems, cryptanalysis and basic tools | | | | |
| 1 | Quantum assumptions and reductions | RUB | 1 | 48 |
| 2 | Algorithm design and implementation of lattice trapdoors | UR1 | 1 | 48 |
| 3 | Classical and quantum cryptanalysis | CWI | 1 | 48 |
| 4 | Side-channel attacks | UR1 | 12 | 48 |
| Work package 4: building blocks for practical advanced protocols | | | | |
| 1 | Lattice-based signatures and other building blocks | ENSL | 9 | 48 |
| 2 | Lattice-based encryption schemes with additional properties | WEI | 9 | 48 |
| 3 | Lattice-based zero-knowledge proofs of knowledge | IDC | 9 | 48 |
| 4 | Implementation of building blocks | RUB | 9 | 48 |
| Work package 5: privacy-preserving protocols | | | | |
| 1 | Anonymous credentials | ENSL | 1 | 48 |
| 2 | Advanced cryptography for e-cash | ORA | 1 | 48 |
| 3 | Advanced cryptography for e-democracy | UPC | 1 | 48 |
| 4 | Implementation of advanced protocols | RHUL | 6 | 48 |
| Work package 6: use cases and demonstrators | | | | |
| 1 | E-voting | SCYTL | 9 | 48 |
| 2 | E-consumer | ORA | 9 | 48 |
| 3 | Anonymous credentials | THA | 9 | 48 |
| 4 | Cyber threat intelligence | TNO | 9 | 48 |

Table 3: List of tasks.

3.2 Partners

The project gathers twelve partners from six countries: seven of the partners are universities and/or research institutes, one is an SME partner and three are industrials. We will briefly summarize their role.

3.2.1 ENSL

As coordinator, ENSL will also lead the Management and Coordination tasks (WP1) and highly participate to the Dissemination tasks (WP2). ENSL will be involved in WP3, WP4 and WP5. In the first one, it will contribute to the analysis of algorithmic problems in lattices and the design of new basic tools for lattice-based cryptography. In WP4, it will provide new lattice-based cryptographic primitives (digital signatures, encryption schemes and zero-knowledge proofs) that will serve as building blocks for the more advanced protocols of WP5. In WP5, it will join the efforts of ORA and UPC in the design of anonymous credentials, e-cash systems and voting protocols.

3.2.2 ORA

ORA will be the technical leader of the PROMETHEUS project. Managing Task 1.2, it will be responsible for fulfilment of the project technical objectives, doing the whole link between WPs. It will also lead WP2 (and in particular Task 2.1) on the dissemination, the standardisation and the exploitation of the scientific results of the project. Regarding technical contributions, Orange will contribute to all WPs, and more specifically on cryptographic building blocks (WP4) and privacy-preserving protocols (WP5). In the WP6, ORA will propose two demonstrators implementing privacy-preserving protocols for e-cash and e-ticketing systems.

3.2.3 CWI

The CWI cryptology group will be mostly involved in WP3, contributing effort toward improved classical and quantum cryptanalysis, and concrete security estimates, as well as algorithmic improvements for lattice trapdoors. Additionally, the group will also contribute to WP4, especially for tasks related to zero-knowledge proofs.

3.2.4 RHUL

The RHUL team will be involved in WP2, WP3, WP4 and WP5. In WP2, the group will lead Task 2.3 on standardization and tracking the NIST process. In WP3, it will contribute to Task 3.3 on the hardness of lattice problems and contribute to Task 3.4 about implementation vulnerabilities and timing attacks on cryptographic implementations. In WP4, it will help in the construction of efficient cryptographic primitives. In WP5, it will lead the implementation task (Task 5.4) and contribute to the construction of advanced cryptographic primitives in the other tasks.

3.2.5 RUB

The RUB team will be involved WP3 and WP4. In WP3, they will contribute to finding general techniques for quantum reductions and they will contribute to the analysis of algorithmic problems in lattices and the design of new basic tools for lattice-based

cryptography. In WP4, they will implement and evaluate lattice-based schemes proposed by the PROMETHEUS team at different security levels for a range of different target platforms.

3.2.6 SCYTL

The tasks of SCYTL in this project are focused on the design and implementation of a demonstrator of the first lattice-based e-voting solution offering long-term privacy in WP6, for which SCYTL is the coordinator. In this context, SCYTL will participate on the provision and evaluation of both functional and implementation-level requirements for lattice-based cryptographic primitives in WP4. In WP5, SCYTL will participate in the research and design of lattice-based cryptographic protocols for e-government solution.

3.2.7 THA

THA provided a lattice-based signature scheme to the NIST upcoming competition, which is a contribution to WP2. In WP3, it will contribute in two points: by trying to make lattice trapdoors more efficient in space and speed, and by analyzing side-channel resistance of lattice-based schemes. In WP6, it will lead the Task 6.4 and provide a software demonstrator for the use anonymous credentials.

3.2.8 TNO

TNO will contribute to build privacy-preserving cryptographic protocols in WP5, based on the building blocks from WP3 and WP4. These protocols are applied to specific uses cases in WP6. As a contributor of WP5, TNO will work on privacy-preserving cryptographic protocols. Furthermore, TNO brings in the use case “Cyber threat intelligence”, which allows parties to jointly derive information on cyber threats, without leaking sensitive information.

3.2.9 UPC

In WP4, UPC will contribute by doing research on lattice-based encryption, signature and zero-knowledge protocols satisfying the necessary requirements to be used in the applications contained in WP5. UPC is leading WP5 and Task 5.3 on the use of lattice-based cryptographic tools for e-democracy, and will work so that the goals of this WP and task are achieved. Furthermore, UPC will contribute to other tasks of WP5. UPC will help SCYTL in the implementation and validation of the e-voting prototype during WP6.

3.2.10 UR1

The EMSEC team will be responsible for the Task 3.2 about the algorithm design and implementation of lattice trapdoor, Task 3.4 about the analysis of side-channel attacks and Task 5.1 about anonymous credentials. The team will also lead the WP4 on building blocks for practical advanced protocols.

3.2.11 WEI

Zvika Brakerski’s research group will be involved in the theoretical aspects of these WPs, collaborating as needed with the other partners. Specifically, in WP3 the group

will contribute to the study of the computational hardness of lattice problems. In WP4 the group will spearhead the efforts for constructing new lattice based encryption scheme. In the context of WP4, the group will also participate in the design of lattice based signature schemes.

3.2.12 IDC

Alon Rosen's research group FACT (Foundation and Applications of Cryptographic Theory) from IDC has extensive knowledge and research experience in cryptographic protocols in general, and lattice-based cryptography in particular, specifically in the areas that are addressed by WP4 and WP5 of PROMETHEUS project. Members of the group will be involved in both the theoretical aspects of these WPs (core of the cryptographic constructions), and the way to go from these theoretical cryptographic algorithms to practical systems that will be used in WP6 and final demonstrators. For this purpose, IDC's researchers will collaborate as needed with the other partners (with Zvika Brakerski, Ronald Cramer, Leo Ducas, Eike Kiltz, Benoit Libert, Kenny Paterson and Damien Stehle on studying new approaches for lattice-based ZK protocols with improved efficiency, and their adaptation to efficient lattice-based voting schemes, possibly in collaboration with SCYTL). In WP4 the group will contribute and lead the efforts for constructing new (and further optimizing and adapting existing) lattice-based zero-knowledge protocols, and in WP5, the group will participate in the design of lattice-based voting schemes.

3.3 Team management

Project Management ensures that the work of the scientific and technological researchers / developers will stay focused on scientific and technological tasks, while an overall administrative synergy is achieved at the same time. The Project Management team will review the project and discuss the technical progress and eventually emerging administrative issues. The project management team is composed by six participants with a specific role. These roles will help to coordinate the different aspects of the project that are not specific to a WP. These six participants are the main contacts with the European Commission.

3.3.1 Project Coordinator

The Project Coordinator (Benoit Libert, ENSL) is responsible for all aspects of the interface between the project and the European Commission. It is the focal point for all administrative contents of the project and will provide assistance for the organization of General Assembly (see Section 3.4.1) and Executive Board (see Section 3.4.2) meetings, support project administration and reporting (including aspects of finances and payment), provide a help desk for partners, cater for user account management of Internet-based cooperation tools and support external event management and communications. The Project Coordinator addresses all project management issues and ensures that the project meets or exceeds its stakeholders' expectations. Further it takes care of the contract management to administer the Grant Agreement and the Consortium Agreement as well as acting as a trustee for the project funds. He will oversee the promotion of gender equality in the project, the science and society issues, related to the research activities conducted within the project. The Project Coordinator will work in close cooperation with the Technical Leader and WP leaders with the

purpose of ensuring a prompt and effective response to all the difficulties that could arise, and ensure that all the milestones are met in the proper scheduling.

3.3.2 Technical Leader

The Technical Leader (Sébastien Canard, ORA) is responsible for ensuring that the project's technical objectives are met with respect to the selected application fields and supervises the overall technical content in this regard. As chairman of the Executive Board (see Section 3.4.2), the Technical Leader will set the baseline for technological assumptions of the project, schedule technical meetings if appropriate and needed and take the lead in technical decisions. It will monitor the overall technical progress and quality of deliverables and lead any discussion that may require mediation.

3.3.3 Ethical and Privacy Issues Manager

The Ethical and Privacy Issues Manager (Damien Stehlé, ENSL) will be responsible for ensuring that all measures have been taken into consideration for the project to timely recognise, analyse and tackle potential ethical and privacy issues deriving from project's activities and project's outcomes.

3.3.4 Dissemination Manager

The Dissemination Manager (Adeline Roux-Langlois, UR1) will be responsible for maximizing the impact of PROMETHEUS and ensure that its results are effectively and widely disseminated, in order to raise awareness, understanding and common acceptance of the project's outcomes at the disposal of the stakeholders.

3.3.5 Exploitation Manager

The Exploitation Manager (Olivier Sanders, ORA) will be responsible for the exploitation strategy and the related business plan that will be followed to exploit the PROMETHEUS results. In addition, the Exploitation Manager is responsible for screening and managing the intellectual property rights.

3.3.6 Gender and Equal Opportunity Manager

The Gender and Equal Opportunity Manager (Octavie Paris, ENSL) will be responsible to oversee that gender issues are appropriately addressed within the framework of the project and that equal opportunities are provided between men and women. In line with the EU directives, special emphasis will be given in the gender issues and appropriate actions will be taken in the beginning and through the duration of the project. With the aim to rectify imbalances between women and men and to enhance a gender dimension in research, approximately 25% of the PROMETHEUS Consortium consists of women. The PROMETHEUS objectives related to gender equality are to

- balance the participation of women and men at all research and innovation levels,
- ensure an equal consideration to applications from women and men,
- empower women to take on management roles in the project,
- provide equitable women and men decision-making process,

- ensure women’s representation in equal measure in public relations materials, and
- encourage women and men to equally attend several project events and activities.

3.3.7 Quality Manager / Project Manager

The Quality Manager, or Project Manager, (Laurent Grémy replaced since May 2019 by Octavie Paris, ENSL) will be responsible for ensuring the quality standards of PROMETHEUS. Along with the Project Coordinator, the Technical Leader and the representative WP Leader, he will be in charge of approving the release of all deliverables. He will organise the deliverable internal review by a dedicated internal deliverable reviewer pool (see Section 5.2) which will ensure their highest quality. In close cooperation with either the Project Coordinator and the Technical Leader, the Project Manager is also in charge of the concrete instantiation of the missions of the Project Coordinator to ensure the good execution of the different stages of the project.

| Role | Participant |
|--------------------------------------|--------------------------------|
| Main roles | |
| Project Coordinator | Benoît Libert (ENSL) |
| Technical Leader | Sébastien Canard (ORA) |
| Ethical and Privacy Issues Manager | Damien Stehlé (ENSL) |
| Dissemination Manager | Adeline Roux-Langlois (UR1) |
| Exploitation Manager | Olivier Sanders (ORA) |
| Gender and Equal Opportunity Manager | Octavie Paris (ENSL) |
| Project Manager | Octavie Paris (ENSL) |
| WP leaders | |
| WP1 | Benoît Libert (ENSL) |
| WP2 | Sébastien Canard (ORA) |
| WP3 | Léo Ducas (CWI) |
| WP4 | Adeline Roux-Langlois (UR1) |
| WP5 | Javier Herranz (UPC) |
| WP6 | Jordi Puiggali Allepuz (SCYTL) |
| WP7 | Damien Stehlé (ENSL) |

Table 4: PROMETHEUS roles

3.3.8 Other leaders

In addition to these seven participants, each WP and task is led by a leader who verify that the purposes of the WP are reached.

WP Leaders. The WP Leaders will be responsible for the technical management and day-to-day running of their work packages, as well as the accomplishment of WP milestones and the delivery of WP deliverables.

Task Leaders. Each task within each WP will be coordinated by an individual participant. For many tasks, two or more participants may be involved. This will happen

in case there is the need to combine different sorts of expertise for the execution of the tasks to the best possible outcome; it may also work as an expression of will and need for closer co-operation. Task leaders will be responsible for timely completion of their tasks and related feedback to the WP leaders.

3.4 Making decision

3.4.1 General assembly

The General Assembly is the highest level of the organization of PROMETHEUS and deals with questions of strategic importance within the project. The General Assembly is responsible for ensuring that the project fulfils its objectives and contractual obligations and enforces the rules of the Grant Agreement and the Consortium Agreement. Responsibilities also include financial decisions (allocation of European Commission funding and any changes related to it) and major changes to research directions in cooperation with the Commission. The Executive Board is responsible for the proper execution and implementation of the decisions of the General Assembly.

3.4.2 Executive board

The Executive Board prepares proposals which the General Assembly needs to carry out its work. It is responsible for monitoring and guiding the scientific work. The Executive Board is composed of WP Leaders and is chaired by the Technical Leader. The Executive Board coordinates the work in the different WPs and helps in resolving any issue that might arise on the basis of the long-term goals of the project, including the exploitation of opportunities. WP Leaders are responsible for coordinating the work carried out and the assigned deliverables as well as for the achievement of the objectives within the WP.

The PROMETHEUS project is helped by two external advisory boards: the Advisory Board for the scientific side of the project, and the External Ethics Committee for the ethic side.

3.4.3 External boards

Advisory Board. The Advisory Board consists of four selected European and non-European organizations not directly involved in the project as partners. It supports and advises project partners with experience and know-how throughout the project duration. Their valuable feedback to the technical process of the project brings many benefits to the project. Members of the Advisory Board will provide an external unprejudiced view without receiving funding from the European Union with respect to the PROMETHEUS project. The Advisory Board will advise on strategic directions of the project in terms of detailed technical goals and impact, comment on the economic feasibility and achieved or missed targets and influence PROMETHEUS long-term targets.

Joppe W. Bos (NXP Semiconductors, Netherlands), Arjen Lenstra (Ecole Polytechnique Fédérale de Lausanne, Switzerland), Tal G. Malkin (Columbia University, USA), and Daniele Micciancio (University of California, USA) stated their interests to guide, support and provide feedback to the PROMETHEUS consortium with advice and expertise throughout the project duration.

External Ethics Committee. The External Ethics Committee is composed of three members, who cover different aspects from an ethical perspective: Bruno Baeriswyl (privacy commissioner of the Canton of Zurich, Switzerland) will bring its expertise most likely for the legal aspects, Nayla Farouki (retired, formerly CEA-Grenoble, France) for the philosophical aspects and Claire Lobet (senior professor at the computer sciences faculty and senior researcher at the CRIDS (Centre de Recherche Droit, Information & Société), Belgium) for the sociological aspects.

3.4.4 Project organization

During the lifetime of the PROMETHEUS project, decisions varying in their nature will be necessary. Most of them will be strategic (relating to the identification of long-term interests) or operational (relating to the day-to-day work). Decisions will be weighted according to their importance and be taken by bodies with the relevant competences. It is not always necessary to involve the Executive Board or even the General Assembly which allows quick and straightforward decision making that facilitates smooth progress of the entire project. In case of more severe decisions, the organizational structure of the PROMETHEUS project allows judgements of different decision makers. One of the major advantages is to include various opinions of experts with different backgrounds and in-depth know-how. Another benefit is that the hierarchical structure makes it possible to weight the judgements of the decision makers by their rank order. The hierarchy and differentiated responsibilities facilitate a clear and straightforward reporting structure which constitutes a considerable advantage in terms of effective collaboration and project progress. Finally, based on the organizational structure the General Assembly is the ultimate decision-making body that has the final say and responsibility (see Figure 2).

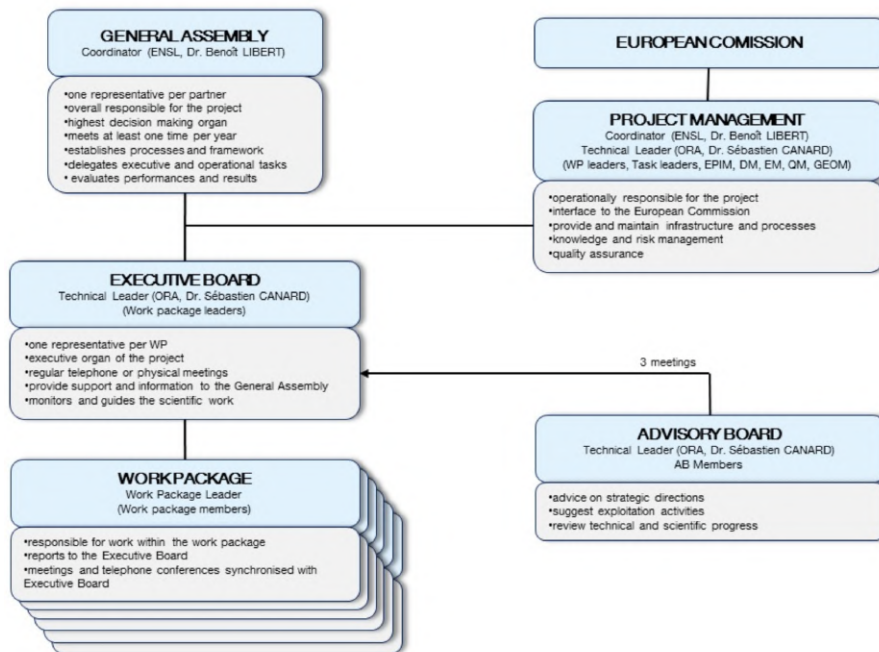


Figure 2: Project organization

3.4.5 Conflict resolution

Each partner undertakes to participate in the efficient implementation of the project and is responsible for cooperating, performing and fulfilling, promptly and on time, all its obligations. In the event that a responsible body identifies a breach by a party of its obligations (e.g., conflict on ownership to results and access rights) the General Assembly is the entity that will monitor the conflict. Conflicts on legal issues which cannot be settled by mutual agreement among the participants or by conflict resolving efforts by the GA, will have to be solved by legal representatives of the involved participants in legal procedures described in the Consortium Agreement. Conflict resolution and decision making procedures will be more fully described in the Consortium Agreement.

4 Quality processes

4.1 Visual identity

The PROMETHEUS consortium has adopted some common processes to increase the visibility of the PROMETHEUS achievements. We have adopted some common rules in order to maximize the visibility of PROMETHEUS inside events: some of them are described in the deliverable 2.2 about dissemination. We have for example provided templates to communicate inside or outside of the project, which follow a unified visual identity, starting with the logo that reflects the goals of PROMETHEUS about privacy.

4.2 Communication

Communication is for sure one of the most essential foundations of successful project collaborations. Therefore we put a lot of effort in the development and constant enhancement of a secure information technology framework.

4.2.1 Internal communication

Email. Subject heading: to ensure efficient recognition of emails, participants have to ensure to always include the name of the project as follow [PROMETHEUS] in the subject title. When sending project related emails, they must include PROMETHEUS in the subject heading followed by a more detailed description of the subject. Attachments: participants consider file size when sending via email. Very large attachments may not be accepted by the recipient server and even modest size attachments might rapidly cause email-quotas to be exceeded, particularly where recipients are away from the office for an extended period. Contact details: participants must provide their contact details (e.g. as email signature) on every mail that you initiate.

Gforge platform. InriaForge is a service offered to facilitate the scientific collaborations of people delivered by Inria. It is an integrated set of tools or components that facilitates « project » collaboration which offers easy access to the best in Git (as well as Subversion), mailing lists, bug tracking, message boards/forums, task management, site hosting, permanent file archival, full backups, and total web-based administration.

Groups and distribution lists. Thanks to the Gforge platform (see above), some groups have been created and each group has its own communication list, as shown in Table 5.

| Group description | Adresse |
|--|--|
| Use case anonymous credentials | prometheuscrypt-acredentials@lists.gforge.inria.fr |
| Mailing list for the commits | prometheuscrypt-commits@lists.gforge.inria.fr |
| List of all the contacts of the PROMETHEUS project | prometheuscrypt-contacts@lists.gforge.inria.fr |
| List for the scientific contacts of PROMETHEUS | prometheuscrypt-contactssci@lists.gforge.inria.fr |
| Main list for the PROMETHEUS project | prometheuscrypt-discuss@lists.gforge.inria.fr |
| Use case e-cash | prometheuscrypt-ecash@lists.gforge.inria.fr |
| Use case e-voting | prometheuscrypt-evoting@lists.gforge.inria.fr |

Table 5: Communication lists

Conference call. Teleconferencing should be used for organising short meetings. The meeting should not exceed 15 participants and the date, time, expected duration, agenda and name of participants should be communicated in advance.

Meetings. Face to face meetings are necessary to maintain relationships between partners, to promote information exchange and to make agreements and major decisions. There are several types of meetings:

- General assembly meetings are plenary meetings and parallel sessions combining technical progress. They take place at least once a year.
- Technical meetings are organised whenever it is needed between the partners (presence of some partner’s representatives according to the subject of the meeting). They may be called by the WP leaders within a WP or between technical WPs in order to coordinate progress on WP level.
- Project review meetings:
 - project reviews may be organised by the EC on request of the EC
 - Physical meetings may be organised for reviewing the reports/progress made and the next steps
 - Presence of the coordinator and WP leaders is required
 - Reviewers appointed by the EC may be present in the review meetings

Meeting minutes. It is the responsibility of the chair of the meeting together with the EB to organise the taking of the minutes. The draft minutes shall be sent to the WP leaders and coordinator within 10 calendar days of the meeting. A deadline will be sent for comment and if no comment is received by the deadline (within a maximum of 15 days after receipt), the minutes will be considered as approved. The minutes are a permanent record of the meeting and will be uploaded on the Gforge platform.

4.2.2 External communication

Communication with the European Commission. All communication between the PROMETHEUS consortium and the European Commission will be channelled through the project coordinator exclusively.

Project website. PROMETHEUS website structure has been designed to target 3 main goals:

- Project communication and presentation of the project progress to the European Commission and all the related stakeholders
- To promote the project results dissemination
- To develop a communication and dissemination plan guaranteeing the technical, market and public coverage of the project results

It can be found at <http://www.h2020prometheus.eu/>.

General requirements In all the project dissemination documents/publications, it is requested to indicate that the project has received funding from the European Union, using the following:

- display the EU emblem (For more information about the use of the EU flag, please refer to the EC publication website);
- include the following text “This project (PROMETHEUS) has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement number 780701”;
- include the project logo which is available on the Gforge platform and on the website (see Figure 3).



Figure 3: PROMETHEUS logo

4.3 Publications

The scientific publications of PROMETHEUS will be published at international journals or conferences which agree to a peer-review system. This ensure either a good visibility and the quality of these publications. A sample of relevant conferences that implement this process are: CRYPTO, EUROCRYPT, ASIACRYPT, ACM CCS (conference on Computer and Communications Security of the Association for Computing Machinery), PKC (Public Key Cryptography), TCC (Theory of Cryptography Conference), ESORICS (European Symposium on Research in Computer Security), Financial

Crypto, PQCrypto (conference on Post-Quantum Cryptography), E-VOTE-ID (conference on Electronic Voting), ICEDEG (International Conference on eDemocracy & eGovernment) and IEEE (Institute of Electrical and Electronics Engineers) Workshop on Information Forensics and Security.

In addition to the scientific publications, the NIST process about the standardization of post-quantum schemes is also peer-reviewed, either by academics and governmental agencies. Nine schemes were submitted by seven partners of the PROMETHEUS project. The reference implementation of these schemes can be freely downloaded on the NIST web page.

In addition, some software developed inside the PROMETHEUS project are available over some free licenses, as the FPLLL software. The software that are under a copyright licence may be evaluated either internally (e.g., ethical hacking) or externally (e.g., by computer security specialists, as ANSSI or CESTI in France).

4.4 Deliverables and milestones

4.4.1 Deliverables

The life of a WP is punctuated with deliverables. These deliverables allow to verify if the project goes in the right direction, share useful information between the participants of the project and even to the scientific / industrial community if a deliverable is public. As Figure 1 shows, the dependency between WP4, WP5 and WP6 will extensively use the deliverables of the other WPs (especially WP3). The list of deliverables is given in Table 6.

| No. | Title | Lead beneficiary | Dissemination level | Due date |
|--|---|------------------|---------------------|----------|
| Work package 1: management and coordination | | | | |
| D1.1 | Project quality plan | ENSL | Public | 9 |
| D1.2 | Internal management report (1) | ENSL | Internal | 12 |
| D1.3 | Internal management report (2) | ENSL | Internal | 24 |
| D1.4 | Internal management report (3) | ENSL | Internal | 36 |
| D1.5 | Risk assessment plan | ENSL | Internal | 12 |
| D1.6 | Project legal and ethical framework (1) | ENSL | Internal | 6 |
| D1.7 | Project legal and ethical framework (2) | ENSL | Internal | 18 |
| D1.8 | Project legal and ethical framework (3) | ENSL | Internal | 36 |
| D1.9 | Project legal and ethical framework (4) | ENSL | Internal | 48 |
| Work package 2: dissemination, standardisation and exploitation | | | | |
| D2.1 | Project website | ENSL | Public | 3 |
| D2.2 | Dissemination plan | ENSL | Public | 3 |
| D2.3 | Intermediate business plane and exploitation report | ORA | Public | 24 |

| No. | Title | Lead beneficiary | Dissemination level | Due date |
|--|---|------------------|---------------------|----------|
| D2.4 | Final business plan and exploitation report | ORA | Public | 48 |
| Work package 3: computational problems, cryptanalysis and basic tools | | | | |
| D3.1 | Survey on computational problems, cryptanalysis and basic tools | RUB | Public | 10 |
| D3.2 | Intermediate results on computational problems, cryptanalysis and basic tools | UR1 | Public | 24 |
| D3.3 | Final results on computational problems, cryptanalysis and basic tools | CWI | Public | 48 |
| Work package 4: building blocks for practical advanced protocols | | | | |
| D4.1 | Survey of existing building blocks for practical advanced protocols | ENSL | Public | 10 |
| D4.2 | Intermediate results on building blocks for practical advanced protocols | WEI | Public | 24 |
| D4.3 | Implementation of building blocks for practical advanced protocols | RUB | Internal | 36 |
| D4.4 | Final results on building blocks for practical advanced protocols | | Public | 48 |
| Work package 5: privacy-preserving protocols | | | | |
| D5.1 | Survey of existing privacy-preserving cryptographic protocols | ORA | Public | 10 |
| D5.2 | Intermediate results on privacy-preserving cryptographic protocols | TNO | Public | 24 |
| D5.3 | Implementation of privacy-preserving cryptographic protocols | RHUL | Internal | 36 |
| D5.4 | Final results on privacy-preserving cryptographic protocols | UPC | Public | 48 |
| Work package 6: use cases and demonstrators | | | | |
| D6.1 | E-voting use case requirements | SCYTL | Internal | 16 |
| D6.2 | E-consumer use case requirements | ORA | Internal | 16 |
| D6.3 | Anonymous credential use case requirements | THA | Internal | 16 |

| No. | Title | Lead beneficiary | Dissemination level | Due date |
|--|--|------------------|---------------------|----------|
| D6.4 | Cyber threat intelligence use case requirements | TNO | Internal | 16 |
| D6.5 | E-voting use case specifications | SCYTL | Internal | 36 |
| D6.6 | E-consumer use case specifications | ORA | Internal | 36 |
| D6.7 | Anonymous credential use case specifications | THA | Internal | 36 |
| D6.8 | Cyber threat intelligence use case specifications | TNO | Internal | 36 |
| D6.9 | E-voting use case demonstrator | SCYTL | Internal | 42 |
| D6.10 | E-consumer use case demonstrator | ORA | Internal | 42 |
| D6.11 | Anonymous credential use case demonstrator | THA | Internal | 42 |
| D6.12 | Cyber threat intelligence use case demonstrator | TNO | Internal | 42 |
| D6.13 | E-voting case evaluation and validation | SCYTL | Public | 48 |
| D6.14 | E-consumer case evaluation and validation | ORA | Public | 48 |
| D6.15 | Anonymous credential case evaluation and validation | THA | Public | 48 |
| D6.16 | Cyber threat intelligence case evaluation and validation | TNO | Public | 48 |
| Work package 7: ethics requirements | | | | |
| D7.1 | Protection of personal data | ENSL | Internal | 12 |

Table 6: List of deliverables

4.4.2 Milestones

Milestones are control points where decisions are needed with respect to a next stage within the project. A milestone may occur when a major result has been achieved, if its successful attainment is required for the next phase of work. Table 7 gives the milestones that have been defined.

4.5 Meetings

4.5.1 Making decision

During the lifetime of the PROMETHEUS project, decisions varying in their nature will be necessary. Most of them will be strategic (relating to the identification of long-term interests) or operational (relating to the day-to-day work). Decisions will be weighted according to their importance and be taken by bodies with the relevant competences. It is not always necessary to involve the Executive Board or even the

General Assembly which allows quick and straightforward decision making that facilitates smooth progress of the entire project. In case of more severe decisions, the organizational structure of the PROMETHEUS project allows judgements of different decision makers. One of the major advantages is to include various opinions of experts with different backgrounds and in-depth know-how. Another benefit is that the hierarchical structure makes it possible to weight the judgements of the decision makers by their rank order. The hierarchy and differentiated responsibilities facilitate a clear and straightforward reporting structure which constitutes a considerable advantage in terms of effective collaboration and project progress. Finally, based on the organizational structure the General Assembly is the ultimate decision-making body that has the final say and responsibility.

| No. | Title | Lead beneficiary | WP | Due date |
|-----|--|------------------|---------------|----------|
| 1 | Successful project start | ENSL | 1 | 1 |
| 2 | End of technical survey | ORA | 3, 4 and 5 | 10 |
| 3 | Use case definition | SCYTL | 6 | 16 |
| 4 | First cryptographic specifications | ORA | 3, 4 and 5 | 24 |
| 5 | First results on cryptographic foundations | CWI | 3 | 36 |
| 6 | Cryptographic APIs and first prototype | RUB | 3, 4 and 5 | 36 |
| 7 | Use case demonstrator | THA | 3, 4, 5 and 6 | 48 |
| 8 | Ethical clearance | ENSL | 1, 2, 6 and 7 | 12 |

Table 7: List of milestones.

Furthermore the PROMETHEUS consortium plans regular telcos and video-telcos, see Table 8. The virtual meetings are planned in parallel to the face-to-face meetings. Face-to-face meetings are needed because of the complexity and large number of interfaces to be developed within this project.

To make important decisions for the entire consortium, project votes will be necessary. Such a vote is either being taken directly in a face-to-face meeting or via telephone conference. Each partner has one vote. Partners directly affected by the vote have veto rights. The Coordinator is responsible for tracking and compiling the votes and providing clear instructions on what is being voted on and how to proceed. Further details on voting rules and attendance requirements will be defined in the Consortium Agreement.

4.5.2 Problem solving

The project's conflict management strategy is achieved through the following key goals:

- Discover and resolve issues before they become serious conflicts,
- Create a climate of trust where partners feel free to exchange any ideas,
- Encourage and engage partners to speak their minds and without hidden agendas.

| Instance | Meeting frequency | Participants |
|---------------------------|--------------------------|---|
| Project management | Bimonthly | Members of the project management, mainly Project Coordinator, Technical Leader, Quality Manager |
| General Assembly | Yearly | One delegate for each partners |
| Executive Board | Biannual | Technical Leader and WP leaders |
| Advisory Board | 3 meetings | Project Coordinator, Technical Leader, WP leaders and members of the Advisory Board |
| WP | Quarterly | Participants of the WP |
| External Ethics Committee | 3 meetings | Project Coordinator, External Ethics Committee members, leaders of the demonstrators and Ethical and Privacy Issues Manager |

Table 8: PROMETHEUS meetings.

The three key activities are organised as follows:

- Review the current project progress at periodic meetings to be able to detect any possible problems before they arise,
- Create a list of activities (list of issues to be solved) where project issues are captured and their status (open, under investigation, deferred, fixed etc.) is remembered,
- Monitor issues through an issue management process, consisting of: detection, recording, analysing, prioritising and allocating ownership of issues.

The following problem escalation path (to be solved at the lowest level, when possible) is defined as follows:

Partner → WP Leader → Executive Board → European Commission

5 Quality assurances

5.1 Management reports

5.1.1 Reporting periods

There are 3 official reporting periods during the project lifetime:

- period 1 from 01/01/2018 to 30/06/2019 (M1-M18);
- period 2 from 01/07/2019 to 31/12/2020 (M19-M36);
- period 3 from 01/01/2021 to 31/12/2021.

5.1.2 Reporting calendar

| Report type | Period | Month | Deadline |
|------------------------------|-----------------------|---------|------------|
| Internal management report 1 | 01/01/2018-31/12/2018 | M1-M12 | 31/12/2018 |
| Periodic Report 1 | 01/01/2018-30/06/2019 | M1-M18 | 30/08/2019 |
| Internal management report 2 | 01/01/2019-31/12/2019 | M12-M24 | 31/12/2019 |
| Periodic report 2 | 01/07/2019-31/12/2020 | M19-M36 | 28/02/2021 |
| Internal management report 3 | 01/01/2020-31/12/2020 | M25-M36 | 31/12/2020 |
| Periodic report 3 | 01/01/2021-31/12/2021 | M37-M48 | 28/02/2021 |
| Final report | 01/01/2018-31/12/2021 | M1-M48 | 28/02/2021 |

Table 9: Reporting calendar

5.1.3 Periodic reports

The consortium will submit a Periodic Report at the end of each period of the project (M18, M36, and M48) to the Commission containing the following:

- publishable summary;
- project objectives for the period;
- work progress and achievements during the period;
- deliverables and milestones tables;
- details of Project Management activities;
- financial statement (Form C) from each partner including an explanation of use of resources;
- audit certificates (if required).

The Periodic Report must be submitted by the coordinator within 60 days following the end of each reporting period. It contains the periodic technical and financial reports.

The periodic technical report consists of two parts:

1. Part A of the periodic technical report contains the cover page, a publishable summary and answers to the questionnaire covering issues related to the project implementation and the economic and social impact, notably in the context of the Horizon 2020 key performance indicators and the Horizon 2020 monitoring requirements. Part A is generated by the IT system. It is based on the information entered by the participants through the periodic report and continuous reporting modules of the electronic exchange system in the Funding & tender opportunities portal. The participants can update the information in the continuous reporting module at any time during the life of the project.
2. Part B of the periodic technical report is the narrative part that includes explanations of the work carried out by the beneficiaries during the reporting period. Part B needs to be uploaded as a PDF document following the template of Part B Periodic Technical report.

The periodic financial report consists of:

- individual financial statements (Annex 4 to the GA) for each beneficiary;
- explanation of the use of resources and the information on subcontracting and in-kind contributions provided by third parties from each beneficiary for the reporting period concerned;
- a periodic summary financial statement including the request for interim payment.

Preparation and submission of periodic report

- Continuous reporting functionality in the participant portal: it is activated at the time the project starts and it is continuously open for the beneficiaries to submit deliverables, to report on progress in achieving milestones, to follow up of critical risks, ethics issues, publications, communications activities, and the answers to the questionnaire on horizontal issues. Periodic reporting functionality in the Funding & tender opportunities portal: following the end of each reporting period the functionality of periodic reporting in the Participant Portal will be activated. While the periodic reporting session is open in the electronic exchange system:
- Each participant will be able to complete on-line their own Financial Statement (and the financial report of their Third Parties, if any) including the explanations on the use of resources;
- Coordinator will be able to upload the Part B of the periodic technical report as a PDF document. When the coordinator submits the periodic report, the IT tool will capture the information from the continuous reporting module in order to generate the Part A of the periodic technical report. The IT tool will consolidate the individual financial statements and it will generate automatically the report with explanations of the use of resources and the periodic summary financial statements, which corresponds to the request for payment.

The periodic report template can be found in the EC portal. Once the reports have been submitted, the EC may:

- approve the reports and proceed with the payment;

- “stop the clock” / suspend the time-limit requesting revision / completion of the financial and / or technical reports and / or deliverables;
- reject them giving justification;
- suspend the payment.

5.1.4 Internal management report

The consortium will submit an internal progress report at M12, M24 and M36 to the Commission. These reports will provide a description of the work done by all partners in each WP and the ongoing and future activities that will be undertaken. The related human resources (Person.Month) per partner per WP will be also reported. The internal progress report will have the same structure as the periodic report (please refer to Section 11.3. Periodic reports) without financial statements.

5.1.5 Final report

In addition to the periodic report for the last reporting period, the coordinator must submit the final report within 60 calendar days following the end of the last reporting period. The final report will most probably include the following:

- 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
 - the socio-economic impact of the action.

The project coordinator compiles this final technical report in consultation with the partners.

- a ‘final financial report’ containing:
 - a ‘final summary financial statement’ will be created automatically by the electronic European platform, consolidating the individual financial statements of the partners for all reporting periods
 - a ‘Certificate on the Financial Statements’ for each partner (and for each linked third party), if it requests a total contribution of EUR 325 000 (or more) reimbursement of actual costs and unit costs.

5.2 Review workflow

The project consortium implements a publication process to ensure the quality of deliverables and of any other external publications. It ensures that the intellectual property rights of the partners are adequately attended to. The described process requires the approval of both the Project Management (mainly through the Project Coordinator, the Technical Leader and the Project Manager) and the reviewers external to the WP, before a publication is released. Here, a publication includes all the public dissemination of the PROMETHEUS project (mainly deliverables and blog posts), except the scientific articles. How this review process works in detail is shown in Figure 4.

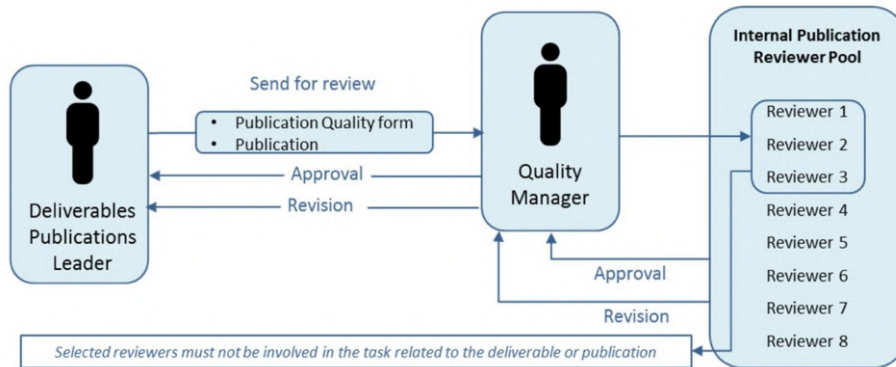


Figure 4: PROMETHEUS reviewing organisation

Since deliverables and other external communication are of different natures, we describe here two different timelines for the review process in Table 10.

| Before the deadline | Action |
|--------------------------|---|
| Beginning of the project | The publication leader, the Technical Leader and the Quality Manager select two to four reviewers |
| 1.5 to 1 month | The Quality Manager send a reminder to the reviewers |
| 3 to 2 weeks | The publication is send to the Quality Manager and the reviewers |
| 1 week | The reviewers and the Quality Manager gives their feedback |
| Deadline | The Quality Manager sent the publication to the European Commission |

(a) Timeline for deliverables.

| Date | Action |
|-----------|---|
| 0 | The publication leader informs the Quality Manager, the WP 2 Leader and the Dissemination Manager of its intention to disseminate |
| < 5 days | If needed, extra reviewers are selected |
| < 10 days | All the reviewers gives their feedback |
| < 14 days | The publication is out |

(b) Timeline for dissemination.

Table 10: Timeline for the review processes.

5.3 Risk management

To guarantee the achievement of the objectives of the PROMETHEUS project, it is essential to identify and understand the significant project risks already in advance. The project communication will be fostered by regular telephone conferences and meetings so that irregularities can be identified and dealt with at an early stage.

The management of risk has been an integral part of the preparation of this project. In a research project we differentiate several types of risk that may or may not materialise:

Technical. Some technical objectives may be in danger or cannot be fulfilled. Key milestones and dependencies have been analysed with regard to these possible risks and have then been taken into account when preparing the time plan and assigning resources.

Schedule. Some risks can cause delays and affect the overall schedule. A thorough planning of dependencies and time spans needed were done throughout the proposal planning process. Small- to medium-sized delays are covered by out planning. Any major delay with impact to our project schedule will be fully tackled by our project procedures.

Cost. Some risks can add cost to the project or envisioned products. Resources needed to perform the tasks were created and verified by each partner independently. Our project organization is fully capable of taking on any financial risks arising during the project duration. All partners are fully aware of their common project responsibility according to EC regulations.

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. Knowing how a risk impacts the project is important as several risks of the same type can be an indication of a larger problem. Few major technical risks connected to the individual WPs and phases of work have been identified in the course of this proposal preparation. As the risks are easier to understand in the technical context of the individual WP, they are described on a WP level in the Table 11 below. To avoid possible negative impact on the project, the corresponding WP leader has proposed risk-mitigation measures for all risks in his WP together with the consortium. Risk management is integrated into the project plan at various levels through monitoring and reviewing processes.

| Description of risk | WP(s) | Proposed risk-mitigation measures |
|---|--------------|--|
| Underperforming partners [Low] | All | Close contact between WP leaders, technical leader and coordinator, short feedback loops and personal contacts (regular Executive Board telcos, physical meetings, etc.) |
| Conflicts between partners (technically and administrative) [Low] | All | Conflict management through close and good contacts, frequent meeting (regular Executive Board telcos/meetings, General Assembly meeting, etc.) |
| Collaboration problems among partners [Low] | All | The Consortium believes that there is extremely low possibility that this could be a risk. Since an “open culture” exists among the partners, problems will be identified and tackled immediately. |
| IPR conflicts between partners or between groups of partners [Medium] | WP1 | Early detection of the issue through close and good contacts, frequent meetings and a clear and unambiguous legal framework (e.g. CA). |

| | | |
|--|-------|---|
| Uncoordinated dissemination activities emergence [Low] | WP2 | The partners will be urged to correlate their activities upon detection of any uncorrelated activities. Clear leadership is needed and experience gained from former projects will be applied to foster common dissemination activities and to funnel any dispersed actions together again. |
| Dissemination/ Exploitation is out of plan [Low] | WP2 | The Task Leader monitors the dissemination/exploitation activities and will interfere immediately. The WP meetings should find workarounds. |
| Most of lattice-based problems are broken [Low] | WP3 | We consider this risk as low as lattice-based computational problems are well-studied for many years. This however may also impact the efficiency of the designed solutions since the size of the parameters may be increased due to some attacks on these problems (see the risk on the efficiency below). |
| Difficulty to find a lattice-based cryptographic solution to a requirement coming from WP5-6 [Low] | WP4-5 | Lattice-based cryptography has been chosen for its maturity on this aspect since a lot of new advanced constructions have been published recently, showing that they have a mathematical structure permitting to obtain advanced properties suitable in the privacy-preserving context. Moreover, the consortium has great skills and experience on the design of advanced cryptographic tools. |
| The design lattice-based privacy-preserving protocols are not enough efficient for implementation in real-life applications [High] | WP5-6 | This aspect will be taken into account at the very beginning of the project. There are moreover some well-known techniques to do pre-computations, or to delegate part of the computation to a more powerful entity. |

Table 11: Risks and mitigation measures

6 Conclusion

The project quality plan has presented the different instances of the PROMETHEUS project and the different roles attributed to participants of the project. In accordance with the Consortium Agreement, the organization of PROMETHEUS will allow to reach the goals set by the consortium, and deal with the possible problems that can arise in such a project.