Aggelos Kiayias—Ed. (UEDIN)
Mirjam Wester (UEDIN)

Y1 Review and Assessment

Deliverable D1.1

31st October 2016
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2016-07-25	AK (UEDIN)	Initial draft
1.0	2016-08-31	AK (UEDIN)	Final version and submission to the EC
1.1	2016-10-26	MW (UEDIN))	Revision after 1st periodic review
1.2	2016-10-27	GD (UCL)	Reviewed and provided feedback
1.3	2016-10-30	BW (SAP)	Review and proof-reading
1.4	2016-10-30	MW (UEDIN)	2nd Review and proof-reading
2.0	2016-10-31	AK (UEDIN)	Revised final version and submission to the EC

Executive Summary

This report, the first of three, encompasses the project activities from September 2015 through to August 2016. It evaluates the project outputs as a whole as well as the achievements and results per work package compared against the description of work (DoA) in more detail. Progress in year one has been mostly in line with the objectives and work plan as specified in the DoA. One of the deviations from the project's plans has been the departure of Mobile Vikings from the consortium. Currently, a new partner is being sought. This report concludes by setting out the directions for the second year.

Contents

1. Introduction

1.1 Purpose of document

The objective of this first year review is to provide an overview the project activities in the first year of the project and provide a basis for moving into second year. We will examine where the consortium was successful and where improvements are needed for the following year.

1.2 Summary of the context and overall objectives of the project

Communicating in a network such as the Internet has the -seemingly- inherent characteristic that anyone observing the network (e.g., a service provider) will get to know the metadata for each connection (including the source and destination, length and size of conversation or data transfer etc.).

This information is a resource that can be exploited and its misuse may have serious implications for the privacy of European citizens especially given the global nature of the Internet. PANORAMIX will develop a European infrastructure for secure communications based on mix-nets which are cryptographic overlays for network communication with the capability to eliminate meta-data information. Furthermore, even though they are a privacy-enhancing technology, mix-nets can also have suitable accountability features by design.

PANORAMIX comes as a response to the need for privacy in a highly connected world where personal information becomes increasingly an item of high valuation and exchange between companies and governments and aims at empowering European citizens in terms of managing their privacy.

In a nutshell the goals of PANORAMIX are the following.

- First, the design, reference and production implementation of a secure mix net system that is freely available, fully documented and interoperable.
- Second, the field demonstration of the system in three use-cases: e-voting (via partner GRNET), big data collection (via partner SAP) and private messaging (via partners Mobile Vikings and Greenhost).

2. First year summary

2.1 Work performed — main results achieved so far

The work performed in the project in the first year can be categorized as follows.

- Investigation of the notion of a mix-net and the supporting technology that is required. This activity is reflected in WP3 and deals with modeling, design and analysis of mix-net systems. The activity of the consortium was quite extensive and is documented in the dissemination report deliverable D2.3. A number of models were considered and evaluated as well as novel concepts in the setting of mix-nets and supporting technologies (including zero-knowledge proofs and blockchain protocols) were investigated.

- Specification of the PANORAMIX mix-net. A substantial amount of effort was invested by the project consortium in order to converge to a specification of the PANORAMIX system. This is reflected in Initial Requirements, Design, and Prototype deliverable D4.1. This document provides background on mix-nets and discusses the design space and the use-cases that are the focal points of the project. It also provides the general API of the mix-net code base to be developed, and provides details of the developmental methodology, tools, and prototyping plan that will be followed.

- Applying the PANORAMIX system for e-voting and e-mail communication. These two applications represent quite opposite sides of the spectrum in terms of requirements for a mix-net. Specifically, e-voting requires mixing that is highly robust, i.e., messages should be guaranteed to be delivered as deposited without any omissions or additions, while responsiveness can be quite low and is acceptable to have high latency in message delivery. On the other hand, e-mail communication has lower requirements in terms of robustness while message delivery is preferable to be quite fast. Deliverables D5.1 and D7.1 outlined the way we envision PANORAMIX would be applied in the setting of e-voting and e-mail communication.

Beyond the above, progress on all tasks of the project has been performed as planned. Figure 2.1 presents the portion of the GANTT chart that corresponds to the project's first year and shows the percentages of completion for each task.

2.2 Milestones reached

In the first year of the project the following milestones were reached:

- (MS1) Panoramix web-site.

- (MS2) Dissemination and exploitation strategy.

- (MS3) Requirements design and prototype.

Year:	Year 1												
Month:	1	2	3	4	5	6	7	8	9	10	11	12	%
WP1: Management													
Task 1.1 – Project Coordination and Communication												D1.1	33
Task 1.2 – Resource Control													33
Task 1.3 – Quality Assurance													33
WP2: Dissemination													
Task 2.1 – Dissemination and Networking		D2.1				D2.2						D2.3	33
Task 2.2 – Standardisation													33
Task 2.3 – Exploitation												D2.5	33
Task 2.4 – Advisory Board													33
WP3: Modelling, Design and Analysis													
Task 3.1 – Mix-nets										D3.1			40
T 3.1.1 – Requirements & Modelling													100
T 3.1.2 – Design													20
T 3.1.3 – Validation & Testing													0
Task 3.2 – Zero-Knowledge proofs													40
T 3.2.1 – Requirements & Modelling													100
T3.2.2 – Design													20
T3.2.3 – Validation & Testing													0
Task 3.3 – Differential Privacy													40
T 3.3.1 – Requirements and Modelling													100
T3.3.2 – Design													20
T3.3.3 – Validation & Testing													0
WP4: Development of Mixnet Infrastructure													
Task 4.1 – Requirements Analysis and Specification									D4.1				33
Task 4.2 – Design													33
Task 4.3 – Validation, Product Implementation and Testing													33
WP5: Pilot Use-case – E-voting													
Task 5.1 – Requirements Analysis and Specification									D5.1				33
Task 5.2 – Design													7
Task 5.3 – Validation, Product Implementation and Testing													4
WP6: Pilot Use-case – Surveys/Statistics													
Task 6.1 – Requirements analysis													100
Task 6.2 – System design and implementation													4
Task 6.3 – Integration with infrastructure													0
Task 6.4 – Validation & Testing													0
WP7: Pilot Use-case – Messaging													
Task 7.1 - Requirements analysis									D7.1				100
Task 7.2 Integration with LEAP software infrastructure													8
Task 7.3 Integration of LEAP with Mobile infrastructure													8
Task 7.4 Testing, Validation and Living Lab													0

Figure 2.1: *GANTT chart for first year and percentages of completion.*

- (MS4) Modeling and design elements report.
- (MS5) The first year report.

3. First year achievements and results

This section sets out the work as it has progressed compared to what was planned in the DoA for each individual WP. Any deviations from the workplan are described. Text taken from the DoA is italicised.

3.1 WP1: Project Management

The lead partner for WP1 is UEDIN.

3.1.1 WP1: Objectives

The project management work package will include all activities that relate to the coordination of the project team and the management of the resources of the project. Specifically our objectives are as follows. Objectives:

- *Provide the global focus on direction and objectives of the project*
- *Coordinating and providing administration of the project work, including management of resources, activities, and deliverables*
- *Ensure a proper level of cooperation, communication, and support the consensus finding within the project work and amongst the project members*
- *Review and track the quality of the work produced within the project*
- *Coordination of project meetings*
- *Maintain the communication with the Project Officer*
- *Coordinate and prepare material for the annual reports to the European Commission*

3.1.2 WP1: Progress towards objectives

Our progress on WP1 was centered around the three tasks that underline the effort of the work package. Task 1.1 is about project coordination and communication. The coordinator liaised all necessary project information with the project officer. The coordinator in collaboration with partner Greenhost setup an installation of the Openproject system in order to provide all necessary logistics support for project management. The Openproject system is used by all partners for version control of deliverables, management of meetings including minutes recording and dissemination. During the course of Y1, the coordinator also liaised with the appointed Ethics Advisor of the consortium, Dr. Joss Wright, and coordinated regarding the Ethics report.

In Task 1.2, resource control was applied by the coordinator and information for financial reports were submitted. In terms of Task 1.3, in the kick-off meeting, the consortium appointed as Quality Assurance Coordinator (QAC) Sacha van Geffen from partner Greenhost.

Regarding inter consortium coordination, we followed our schedule for monthly meetings for the Work Package Leader Board and the Project Steering Committee. Specifically, the following meetings took place in reverse order.

- August 2016 08/30/2016 02:00 PM-03:00 PM WPLB Meeting #12 Location: skype Telco

  Invitees (14): Aggelos Kiayias; Anna Piotrowska; Benjamin Weggenmann; Dimitris Mitropoulos; Florian Kerschbaum; George Danezis; Giorgos Tsoukalas; Harry Halpin; Helger Lipmaa; Michal Zajac; Panos Louridas; Sacha van Geffen; Tariq Elahi; Tatjana Vandenplas

  Attendees (9): Aggelos Kiayias; Benjamin Weggenmann; George Danezis; Harry Halpin; Helger Lipmaa; Michal Zajac; Panos Louridas; Tariq Elahi; Tatjana Vandenplas

- July 2016 07/26/2016 02:00 PM-03:00 PM WPLB Meeting #11 Location: Telco

  Invitees (10): Aggelos Kiayias; Benjamin Weggenmann; Florian Kerschbaum; George Danezis; Harry Halpin; Helger Lipmaa; Joss Wright; Panos Louridas; Tariq Elahi; Tatjana Vandenplas

  Attendees (7): Anna Piotrowska; Benjamin Weggenmann; Harry Halpin; Helger Lipmaa; Joss Wright; Panos Louridas; Tariq Elahi

- June 2016 06/28/2016 02:00 PM-03:00 PM WPLB Meeting #10 Location: Telco

  Invitees (13): Aggelos Kiayias; Anna Piotrowska; Benjamin Weggenmann; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Harry Halpin; Helger Lipmaa; Panos Louridas; Sacha van Geffen; Tariq Elahi; Tatjana Vandenplas

  Attendees (6): Anna Piotrowska; Benjamin Weggenmann; Dirk Moors; Harry Halpin; Panos Louridas; Tariq Elahi

- May 2016 05/31/2016 02:00 PM-03:00 PM WPLB Meeting #9 Location: Teleconference

  Invitees (12): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Harry Halpin; Helger Lipmaa; Panos Louridas; Sacha van Geffen; Tatjana Vandenplas

  Attendees (7): Aggelos Kiayias; Benjamin Weggenmann; George Danezis; Harry Halpin; Helger Lipmaa; Panos Louridas; Tatjana Vandenplas

- April 2016 04/26/2016 02:00 PM-03:00 PM WPLB Meeting #8 Location: Telco

  Invitees (11): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Claudia Diaz; Florian Kerschbaum; George Danezis; Harry Halpin; Helger Lipmaa; Panos Louridas; Sacha van Geffen; Tariq Elahi

  Attendees (5): Anna Piotrowska; Benjamin Weggenmann; Helger Lipmaa; Panos Louridas; Tariq Elahi

  04/25/2016 10:00 AM-11:00 AM WP4 meeting Location: Over skype

  Invitees (8): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Florian Kerschbaum; George Danezis; Giorgos Tsoukalas; Panos Louridas; Tariq Elahi

  Attendees (4): Aggelos Kiayias; Giorgos Tsoukalas; Panos Louridas; Tariq Elahi

- March 2016 03/21/2016 08:00 AM-04:00 PM WPLB - PSC Meeting #7 Location: Saarbrucken - Anreise-Congresshalle

  Invitees (23): Aggelos Kiayias; Anna Piotrowska; Athanasios Angelakis; Benjamin Weggenmann; Claudia Diaz; Daniel Bernau; Dirk Moors; Florian Kerschbaum; George Danezis; Giorgos Tsoukalas; Harry Halpin; Helger Lipmaa; kwadronaut k; Marc Juarez; Mart van

Santen; Meskio Meskio; Michal Zajac; Mooness M; Nikolaos Alexopoulos; Panos Louridas; Rafael Galvez; Sacha van Geffen; Tariq Elahi

Attendees (18): Aggelos Kiayias; Anna Piotrowska; Athanasios Angelakis; Benjamin Weggenmann; Florian Kerschbaum; Giorgos Tsoukalas; Harry Halpin; Helger Lipmaa; Jacques Bus; Joss Wright; Meskio Meskio; Michal Zajac; Panos Louridas; Rafael Galvez; Sacha van Geffen; Sven Heiberg; Tariq Elahi; Varac Varac

- February 2016 02/25/2016 02:00 PM-03:00 PM WPLB - PSC Meeting #6 Location: Telco

  Invitees (12): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Harry Halpin; Helger Lipmaa; Panos Louridas; Sacha van Geffen; Tariq Elahi

  Attendees (7): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Harry Halpin; Helger Lipmaa; Panos Louridas; Sacha van Geffen

- January 2016 01/29/2016 01:00 PM-02:00 PM WPLB Meeting #5 Location: Skype Telco

  Invitees (16): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Claudia Diaz; Daniel Bernau; Dirk Moors; Florian Kerschbaum; George Danezis; Helger Lipmaa; Marc Juarez; Mart van Santen; Michal Zajac; Panos Louridas; Rafael Galvez; Sacha van Geffen; Tariq Elahi

  Attendees (8): Aggelos Kiayias; Athanasios Angelakis; Benjamin Weggenmann; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Tariq Elahi

- December 2015 12/18/2015 01:00 AM-02:00 AM WPLB Meeting #4 Location: SAP Telco

  Invitees (9): Aggelos Kiayias; Benjamin Weggenmann; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Sacha van Geffen

  Attendees (8): Aggelos Kiayias; Benjamin Weggenmann; Claudia Diaz; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Sacha van Geffen

- November 2015 11/27/2015 01:00 PM-02:00 PM WPLB meeting #3 Location: SAP Telco

  Invitees (8): Aggelos Kiayias; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Sacha van Geffen

  Attendees (5): Aggelos Kiayias; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas

- October 2015 10/30/2015 01:00 PM-02:00 PM WPLB meeting #2 Location: SAP Telco

  Invitees (8): Aggelos Kiayias; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Sacha van Geffen

  Attendees (7): Aggelos Kiayias; Claudia Diaz; Florian Kerschbaum; George Danezis; Helger Lipmaa; Panos Louridas; Sacha van Geffen

- September 2015 09/25/2015 01:00 PM-02:00 PM WPLB meeting #1 Location: Skype

  Invitees (5): Aggelos Kiayias; Claudia Diaz; George Danezis; Helger Lipmaa; Panos Louridas

  Attendees (5): Aggelos Kiayias; Claudia Diaz; George Danezis; Helger Lipmaa; Panos Louridas

  09/03/2015 07:00 AM-07:00 AM Kick-off Meeting Location: Athens - Caravel Hotel

  Invitees (9): Aggelos Kiayias; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Giorgos Tsoukalas; Helger Lipmaa; Panos Louridas; Sacha van Geffen

  Attendees (9): Aggelos Kiayias; Claudia Diaz; Dirk Moors; Florian Kerschbaum; George Danezis; Giorgos Tsoukalas; Helger Lipmaa; Panos Louridas; Sacha van Geffen.

3.1.3 WP1: Deviation from objectives

Difficulties in coordination and quality assurance arose from the availability limitation of Sacha Van Geffen from partner Greenhost. The task of quality assurance control fell back to the coordinator while a new leader of WP7 was sought. Dr. Harry Halpin, initially a member of our advisory board, stepped in and was contracted by partner Greenhost to assume the leadership role in WP7. Regarding partner UoA, post-doctoral researcher A. Angelakis became ill and stopped participating in the project activities. The budget committed to Dr. Angelakis was recovered and is still available to the consortium.

3.1.4 WP1: Beneficiary involvement

UEDIN (lead) lead this work package and contributed to both tasks by carrying out the coordination, planning, management and administration of activities.

UoA offered logistics support specifically in managing the OpenProject system.

UCL devoted time to cross WP quality control of deliverables (Task 1.3).

Table 3.1 shows the use of resources for WP1 in Y1.

Partner	Work Package 1	
	PMs completed in Y1	Total PMs
UEDIN	2.72 ✓	7.2
UCL	1.08 ✓	5.4
UT	0 ✓	0
KU Leuven	0 ✓	0
GRNET	0 ✓	0
SAP SE	0 ✓	0
Greenhost	0 ✓	0
Mobile Vikings	0 ✓	0
UoA	0 ×	14
Total	**3.8** ✓	**26.6**

Table 3.1: Use of resources in Y1 for WP1. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.1.5 WP1: Documents and Deliverables produced

- D1.1 : Y1 Review and Assessment
- D1.4 : Ethics report

Deliverable D1.1 was delivered on time (31/08/2016). However, it was rejected after the first periodic review. D1.1 was resubmitted taking all the reviewers' comments into account on 31/10/2016. Deliverable D1.4 was submitted on 31/08/2016, a month later than the planned due date after permission was given by the program officer. It was also rejected after the first periodic review. D1.4 was resubmitted taking all the reviewer's comments into account on 31/10/2016.

3.2 WP2: Dissemination

The lead partner for WP2 is UEDIN.

3.2.1 WP2: Objectives

The WP2 main objectives are:

- *To promote project activities and outcomes and create a wide impact.*
- *To disseminate the project results via participation in public events, submission of papers and public documents to conferences, journals, magazines and editorial initiatives promoted by the Programme, the Commission, a project cluster or any cross-programme actions.*
- *To present and publish technical results of the project at scientific and policy events.*
- *To raise awareness of the achieved results by reaching broader user communities*
- *Formulate exploitation strategies that enable optimal exploitation of the project outcomes and ensure maximal economic impact for the EU.*

3.2.2 WP2: Progress towards objectives

The first task of WP2 that we tackled during Y1, was 2.1, dissemination and networking. A dissemination plan was furnished and the project web-site was produced. A dissemination report was produced with the end of the project. Regarding standardisation, task 2.2, a number of initial first steps were made focusing particularly to W3C and IETF. Regarding exploitation, task 2.3, a thorough preliminary exploitation report was prepared and made available with the end of Y1. The advisory board has been formed, as part of Task 2.4, and they were invited to participate in our kick-off in Athens and the first semester meeting in Saarbrucken. Two (different) members of the board were persent in the two meetings: Prof. Bart Preneel from KUL and Prof. Antonis Symvonis in the former and Jacques Bus and Sven Heiberg participated in the latter.

3.2.3 WP2: Deviation from objectives

A particular challenge in this work package was the difficulty of finalising the exploitation plan of partner Mobile Vikings. The partner, shortly after the commencement of the project, was acquired by a larger company in Belgium, Medialaan, and had to undergo a major restructuring of their objectives and business profile. This lead to a number of different scenarios that were explored and an overspending of resources regarding WP2 for this partner. For partner UoA, underspending of resources for the same reason as in WP1, cf. Section 3.1.3, nevertheless other partners (UEDIN) covered all necessary tasks.

3.2.4 WP2: Beneficiary involvement

UEDIN (lead) lead this work package; nevertheless, all partners contributed to the tasks as detailed above and specifically by participating in international conferences, promoting standardization efforts and publishing their work.

UoA offered logistics support specifically in managing the OpenProject system.

UCL participated also on standardization efforts (specification writing and reviews) and on exploitation through deployment and releases of open-source packages.

SAP managed the exploitation report and coordinated with all partners regarding their exploitation strategies.

Table 3.2 shows the use of resources for WP2 in Y1.

Partner	Work Package 2	
	PMs completed in Y1	Total PMs
UEDIN	0.48 ✓	2
UCL	1.3 ✓	6
UT	1.6 ✓	6
KU Leuven	1.5 ✓	5
GRNET	0 ✓	16
SAP SE	4.1 ✓	7
Greenhost	2 ✓	6
Mobile Vikings	4.1 ✓+	6
UoA	0 ×	4
Total	**15.08** ✓	**58**

Table 3.2: Use of resources in Y1 for WP2. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a green "$✓_+$" means overspending of resources, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.2.5 WP2: Documents and Deliverables produced

- D2.1 Public Web Page and Blog (Editor: UEDIN) [Due: M02] A public web page and blog have been created. The deliverable consists of a description thereof.

- D2.2 Dissemination Plan (Editor: KU Leuven) [Due: M06] A dissemination plan has been outlined, where dissemination activities via various channels have been planned as described in Task 2.1.

- D2.3 Dissemination Reports (Editor: KU Leuven) [Due: M12]

- D2.5 Preliminary Exploitation Plan (Editor: SAP) [Due: M12] In this deliverable, the first version of the exploitation plan is presented. It has been aligned with the consortium partners' business plans and market evaluation.

Regarding submission, we note that D2.1 submitted late on 07/06/2016, however note that the website went public on time on 31/10/2015, furthermore D2.2 was available on time internally for the consortium partners but was submitted late on 07/06/2016 after interacting with the program officer regarding the due process of deliverable submission (communication response on May 30th, 2016). Deliverables D2.3 and D2.5 were submitted on time on 31/08/2016.

3.3 WP3: Modelling, Design and Analysis

The lead partner for WP3 is UCL.

3.3.1 WP3: Objectives

This WP proposes technology options, with analysis and early evidence for building mix-nets to inform development (WP4), that serve the needs of the use-cases (WP5, WP6, WP7). Objectives:

- *Task 3.1: (A) Understand the feature set, security and performance trade-offs between re-encryption mix-nets that have been traditionally used for mixing ballots and decryption mix-nets that have been used traditionally for messaging. Study advanced properties such as key rotation, forward secrecy, and resilience to failures.*
- *Task 3.1: (B) Integrate robust-mixing techniques into decryption mix nets, and in particular adapt ideas from randomized partial checking, to provide proofs that messages are delivered correctly.*
- *Task 3.1: (C) Research options for bi-directional anonymous mid-latency messaging, allowing the recipient of an anonymous message to communicate some information back to the anonymous sender. Features should support the gathering of statistics and surveys (to support the needs of WP6). Study designs that require state in mixes, those that allow for stateless relays, and those that allow for frequent key rotation for forward secrecy.*
- *Task 3.2: (A) Study most efficient existing non-interactive zero knowledge (NIZK) shuffle proofs both in the random oracle (RO) model and common reference string (CRS) model. If possible, propose more efficient protocols in either of the two models. Study trade-offs between efficiency and conceptual simplicity.*
- *Task 3.2: (B) Study whether RO model is sufficient/good for shuffle proofs. Study how to employ CRS-based shuffle proofs (methods of trustworthy generation of CRS)*
- *Task 3.2: (C) Provide input to other work packages. This includes both cryptographic know-how but also concrete protocols that may be needed for implementation.*
- *Task 3.3: (A) Use definitions inspired from differential privacy to measure the security and level of assurance provided by mix-nets. Derive, if possible, composable metrics of security that capture the rate of privacy loss over time; specialize, and / or weaken, differential privacy based definition to capture weaker adversaries in the context of mixing (i.e. that may not have full side information; that may only be allowed a bounded number of observations). Re-cast traditional disclosure attack theory in the context of those metrics.*
- *Task 3.3: (B) Combine mix-nets with other privacy mechanism, particularly differentially private ones, to make them more efficient. Show that mixing, with or without cover traffic, may provide a differentially private mechanism that can be used to implement non-communication primitives, such as Private Information Retrieval, Oblivious Transfer or ORAM. Study the trade-offs between the strength of the resulting mechanism and the systems cost of the mix-net.*

3.3.2 WP3: Progress towards objectives

For the first 12 months of the project the team around WP3 has produced work covering a number of core tasks defined in the work package, all contributing directly to its objectives to provide technology options in relation to building mix-nets (WP4), and serve the use cases (WP5-WP7). Some of this progress has been integrating in deliverable D3.1, and some progress is to contribute to future deliverables of WP3, as well as other submitted and future deliverables (WP4-7).

More specifically, the progress per task so far consists of the following work and achievements:

Task 3.1 (A) Panoramix partners have compiled surveys of techniques concerning re-encryption mix networks, and their performance, as well as a wide-ranging survey of technologies relating to decryption mix networks (deliverable D3.1). In terms of resilience to failures partners have collaborated on the design of network level anonymity systems, subject to such failures, with other groups (ETH Zurich) and continue to do so (D3.1, Appendix).

Task 3.1 (B) This task has been on-hold while more basic design and research work is done in relation to mix-nets, before looking at integrating partial-checking into them.

Task 3.1 (C) A design of a mix-net based on multi-party computation (MPC) instead of traditional encryption/decryption was also investigated as a design option (D3.1). A methodology for the traffic analysis of low-latency mix-network and onion routing systems was developed that will be the basis of future design evaluations (D3.1). Partners are also working on systems to gather private statistics from anonymity networks using succinct data structures (D3.1 Appendix).

Besides this, partners are working on a fuller design for a traffic analysis resistant low-latency mix-net, Loopix. This mix-network integrates ideas from mixing, traffic analysis resistance using cover traffic, and low-latency systems to support messaging (for WP7).

Task 3.2 (A) The partners have designed both a more efficient shuffle proof, as well as generic more efficient proofs in the CRS model (D3.1). A clear comparison is provided with previous and related work demonstrating key efficiency advantages. Generic more efficient Succinct Arguments of Knowledge (SNARKs) have also been designed, that could form the basis of more efficient proofs of correct shuffle on the future.

Task 3.2 (B) Panoramix partners did foundational work on designing more efficient CRS based proofs (D3.1). However, the issue of generating CRS securely is still under investigation.

Task 3.2 (C) Partners have provided explicit support to a number of other packages: the shuffle proofs and efficient SNARKs support directly the election use-case (WP5), the private statistics aggregation work supports WP6 and WP7. The design work on MPC based anonymity, evaluation based on traffic analysis, and network level mixing supports WP7. Besides those a number of formal design documents in relation to the secure collection and handling of privacy sensitive data, APIs for mix networks and short-term design options for anonymizing messaging systems were also provided.

Task 3.3 (A) Detailed work on this task is on-going. Currently partners are integrating concepts of differential privacy into the design of mix-nets for messaging. This will be included in the future deliverables of WP3 and WP7.

Task 3.3 (B) Partners have looked at privacy definitions, relating to differential privacy, and their short comings (D3.1) particularly relating to location privacy, which supports WP6. A number of design patterns were identified and further research questions to explore. Statistics gathering systems based on differential privacy have also been designed with anonymity systems/mix-nets telemetry as applications in mind (D3.1).

Besides, the applicability of using mix-networks to implement weaker form of PIR as well as OPRAM are currently being investigated, and will be included in future deliverables.

3.3.3 WP3: Deviation from objectives

So far the tasks defined in the original plan have been well aligned with the work needed and performed. We note that some of the work performed in the first 12 months was too immature

to be included in D3.1, and will be integrated in future deliverables of WP3 or other work packages.

3.3.4 WP3: Beneficiary involvement

The work carried out by each partner closely follows the original plan:

UCL (lead) worked on private statistics and aggregates (supporting WP6), advances in traffic analysis for evaluating mix-networks and low-latency anonymity systems, low-latency designs for messaging (to support WP7), as well as design advice for WP4 and WP7.

UT worked on efficient shuffle proofs, efficient SNARKS and provided an overview of shuffle technologies (supporting WP4 and WP5).

UEDIN/UoA provided designs for mix-nets based on MPC as a design option to support WP4/WP7.

KUL provided a review of existing designs for decryption mix-nets and anonymity systems; and further work on mix-networks for future deliverables.

SAP provided first ideas for integrating utility and privacy within the context of differential privacy (in support of WP6).

Table 3.3 shows the use of resources for WP3 in Y1.

Partner	Work Package 3	
	PMs completed in Y1	Total PMs
UEDIN	0.96 ✓	20
UCL	7.62 ✓	36
UT	18.5 ✓	42
KU Leuven	11.7 ✓	30
GRNET	0 ✓	0
SAP SE	6.06 ✓	12
Greenhost	0 ✓	0
Mobile Vikings	0 ✓	0
UoA	3.5 ✓	12
Total	**48.34** ✓	**152**

Table 3.3: Use of resources in Y1 for WP3. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.3.5 WP3: Documents and Deliverables produced

- D3.1: Modelling and Design Elements Report (Editor: UCL) [Due: M10] Describes some of the existing shuffle protocols (WP3.2), initial design options for mix-nets (WP3.1) and definitions of privacy (WP3.3).

Deliverable D3.1 was delivered on time (30/06/2016). It was however rejected after the first periodic review. D3.1 was resubmitted in revised form, taking all the reviewers' comments into account, on 31/10/2016.

3.4 WP4: Development of Mix-net Infrastructure

The lead partner for WP4 is KUL.

3.4.1 WP4: Objectives

The Work Package pulls technologies from WP3 to build a product that may be customized to serve the purposes of the use cases of WP5, WP6, and WP7. Objectives:

- *Use Cases Realization: Develop a production-capable software infrastructure that will support the mix-net service and all the project's use cases.*
- *Security, Scalability: Address important basic issues, such as security, scalability, and fitness to modern information technology environment comprising cloud computing, mobile devices, and data-driven markets.*
- *Integration: On top of the basic infrastructure, integrate specific infrastructure requirements from the results of WP3 and from the use cases of WP5, WP6 and WP7, while focusing on practical and implementation issues.*
- *Implementation, Testing, Deployment of the integrated mix-net service.*

3.4.2 WP4: Progress towards objectives

Significant progress has been made in capturing the initial requirements and producing a preliminary design to address them. The design is aligned with the aim of realizing the three different use-cases of e-voting, messaging, and statistics and surveys. Also, identified are non-functional requirements concerning security, ease-of-use and adoption. A prototype implementation has been produced according to the preliminary design specs that has been demonstrated for two of the use-cases: e-voting and messaging, showing the viability of the platform as well as the potential for integration of the use-case requirements on top of the current design.

3.4.3 WP4: Deviation from objectives

There is deviation (underspending of resources) only by partner UoA, for the same reason as in WP1, cf. Section 3.1.3, nevertheless other partners (UEDIN) covered all necessary tasks. There have been no other deviations from the original objectives of the WP.

3.4.4 WP4: Beneficiary involvement

This work package requires participation from every partner. A coarse breakdown follows:

UEDIN contributed to the requirements analysis phase as well as contributed to the preliminary design discussion and writeup.

KUL managed the work package by coordinating the partner activities around requirements analysis, design, and prototyping and the resultant writeup in the form of D4.1

UoA contributed to the requirements analysis phase as well as contributed to the preliminary design discussion and writeup.

GRNET provided their expertise in e-voting for the requirements analysis and preliminary design description. They also implemented a prototype system that can demonstrate the creation, and management of a mix-net, and also can provide basic e-voting and messaging functionality.

UT provided feedback about the requirements and the preliminary design.

UCL provided requirements analysis, expert advice on security and privacy in mix-net, and design suggestions for both the general platform as well as the specific use-case of messaging.

GH provided the requirements analysis of the messaging use-case and also related design specifications.

Table 3.4 shows the use of resources for WP4 in Y1.

Partner	Work Package 4	
	PMs completed in Y1	Total PMs
UEDIN	0.24 ✓	16
UCL	2.62 ✓	12
UT	1.6 ✓	12.8
KU Leuven	3.1 ✓	10
GRNET	16.31 ✓	48
SAP SE	0 ✓	0
Greenhost	4 ✓	14
Mobile Vikings	3.2 ✓	8
UoA	0 ✗	30
Total	**31.07** ✓	**150.8**

Table 3.4: Use of resources in Y1 for WP4. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.4.5 WP4: Documents and Deliverables produced

- D4.1: Initial Requirements, Design, and Prototype (Editor: KUL) [Due: M9] The first version of the system that addresses basic concerns in all three tasks that do not depend on other work packages, requirements addressing the state-of-the-art industry environments, design addressing development methodology and tools, and prototype addressing development, deployment, and the testing environment.

Deliverable D4.1 was delivered on 08/06/2016, a week after the expected delivery date (31/05/2016) after obtaining permission from the program officer (e-mail dated May 30th, 2016). It was rejected after the first periodic review. The revised version, taking into account the reviewer's comments, was resubmitted on 31/08/2016.

3.5 WP5: Use-case: E-voting

The lead partner for WP5 is GRNET.

3.5.1 WP5: Objectives

WP5 will deliver an e-voting service supporting large scale elections up to hundreds of thousands of voters on top of the mix-net infrastructure developed in WP4. The e-voting application will be a separate network service, accessible by voters and election officials through multiple devices (desktop computers, tablets, smartphones). The process will be verifiable end-to-end, from the

encryption of ballots at the voter's device, through the mix-net service, and back to the e-voting service for counting. Voters will be able to verify that their vote was indeed counted in the results, and election authorities will have access to suitable proof for the correctness of the process. In particular, the objectives are:

- *Production Quality e-Voting Platform: Develop a production quality e-voting platform able to host large scale elections with hundreds of thousands of voters.*
- *Front-end Service: Develop front-end applications through which voters will be able to cast their votes; the applications will allow voting from different electronic devices, such as desktop computers, tablets, and smartphones.*
- *Usability, Verifiability: Provide easy to use, intuitive means of vote verification, so that voters can easily verify that their vote is properly counted, without compromising its secrecy.*

3.5.2 WP5: Progress towards objectives

WP5 has made good progress in the first year of the project, advancing according to plan. The e-voting service will build on the Zeus e-voting platform (`https://zeus.grnet.gr`) developed by GRNET. In particular, in the first year of the project development focused on:

- Introducing a two-factor authentication mechanism; when enabled, users access the voting booth by both using the voting invitation and proving their credentials.
- Changes in the UI to keep up to date with latest developments in web and mobile.
- Design of the interoperability of the PANORAMIX mix-net, which will be provided by WP3, and the mix-net framework, which will be provided by WP4, with Zeus. Zeus will be one use-case of the PANORAMIX platform. Before the start of the project Zeus used an embedded Sako-Kilian mix-net, with significant shortcomings in speed. Zeus therefore needs to be refactored in order to use the PANORAMIX framework API. The design of the refactoring was a major work component in the first year.

Regarding the last item above, note that work does not need to wait for the actual mix-net to be established by the research partners in WP3. Zeus will be able to work with the API and the platform of WP4, even with the current mix-net; this will allow early testing of the design and implementation choices of the PANORAMIX platform.

3.5.3 WP5: Deviation from objectives

There is deviation (underspending of resources) only by partner UoA, for the same reason as in WP1, cf. Section 3.1.3, nevertheless other partners (UEDIN) covered all necessary tasks. There have been no other deviations from the original objectives of the WP.

3.5.4 WP5: Beneficiary involvement

GRNET (lead) worked as planned in the Work Package.

UoA did not contribute as planned, probably because of the initial problems of splitting work between UoA and UEDIN.

UT contributed to planning the implementation and use of the mix-net that is being designed; it is expected to ramp up significantly from the second year of the project, as the mix-net design itself is finalized.

Table 3.5 shows the use of resources for WP5 in Y1.

Partner	Work Package 5	
	PMs completed in Y1	Total PMs
UEDIN	0 ✓	4
UCL	0 ✓	0
UT	0.5 ✓	16
KU Leuven	0 ✓	0
GRNET	20.62 ✓	62
SAP SE	0 ✓	0
Greenhost	0 ✓	0
Mobile Vikings	0 ✓	0
UoA	0 ✗	14
Total	**21.12** ✓	**96**

Table 3.5: Use of resources in Y1 for WP5. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.5.5 WP5: Documents and Deliverables produced

- D5.1: Requirements and User Interface Design (Editor: GRNET) [M9] Documents including a first version of the e-voting system.

Deliverable D5.1 was delivered on time (08/06/2016) and accepted by the reviewers.

3.6 WP6: Use-case: Survey/Statistics

The lead partner for WP6 is SAP SE.

3.6.1 WP6: Objectives

The objective of this work package is to demonstrate the use and advantages of the mix network in a collaborative (SaaS) application. We collect data (survey answers) from a set of predefined (simulated) clients and aggregate those in a database. Due to the sensitivity of the data (e.g. health, religion, business secrets, etc.) it needs to be strongly protected. Still we want to perform the typical big data type of aggregate analysis on them with reasonable accuracy. The objective of this work package is to equip the database with the necessary mechanisms and connect it to the mix network. We aim three non-functional goals: anonymity, data confidentiality and performance. In our business scenario customers are often asked for sensitive data. For example, they might provide feedback on the cloud service provider and they may be reluctant to provide negative feedback, since they are dependent on the longterm business relationship. Another example is pricing information that could be abused by competitors or customers. Anonymity removes the link to the data owner and hence encourages reporting, free from fear of retaliation. We expect more honest answers in surveys improving their accuracy. Still, in certain situations like an outstanding small or large company the data values themselves may reveal the data owner. Hence we use data confidentiality in order to protect them as well. Last, but not least, we need performance to handle the large volumes of data in our scenario. In summary, our non-functional goals are as follows: Objectives

- *Anonymity: The client should stay anonymous among the group of survey participant, i.e. the identity of the owner of a data value should be indistinguishable among the k participants.*

- *Data Confidentiality: The data of an individual client should not be discernible from the aggregates. In particular we aim at an adversary not being able to distinguish whether the data of an individual was among the input set in the first place.*

- *Performance: Our system should be able to scale easily to volumes of data present in current day data centres. Evaluation of already collected should be quick and almost instant.*

3.6.2 WP6: Progress towards objectives

In the first year, we have been working on the requirements analysis task T6.1. For this, we have connected with experts from other SAP units and identified suitable business cases that match the survey/statistics scenario in WP6. We have discussed their needs and distilled common requirements for the demonstrator. Furthermore, we have identified requirements regarding ease-of-use and flexibility of mix-nets.

In addition to that, we have performed experiments with differentially private mechanisms to determine their effect on the quality of results in privacy-preserving data analysis (privacy-vs-utility tradeoff). This will help us in the selection of the right mechanisms and choice of parameters in the design phase of the work package.

3.6.3 WP6: Deviation from objectives

There have been no deviations from the original objectives of the WP. Depending on the example business case that will serve as basis for the demonstrator, we will determine further concrete instantiations of our requirements, which will also be included in deliverable D6.1.

3.6.4 WP6: Beneficiary involvement

SAP In the role of task lead for T6.1, SAP connected with product owners and stakeholders to analyze requirements for the WP6 demonstrator from their business cases.

UCL researched the extent to which existing private statistics collection and aggregation methods could be used to collect more complex aggregates in mix networks, such as medians and percentiles of distributions.

UT undertook initial research on differential privacy to better understand the topic and requirements.

Table 3.6 shows the use of resources for WP6 in Y1.

3.6.5 WP6: Documents and deliverables produced

No deliverables were planned for Y1.

3.7 WP7: Use-case: Messaging

The lead partner for WP7 is Greenhost.

Partner	Work Package 6	
	PMs completed in Y1	Total PMs
UEDIN	0 ✓	4
UCL	3.69 ✓	18
UT	0.5 ✓	4
KU Leuven	0 ✓	0
GRNET	0 ✓	0
SAP SE	7.93 ✓	35
Greenhost	0 ✓	0
Mobile Vikings	0 ✓	0
UoA	0 ✓	0
Total	**12.03** ✓	**61**

Table 3.6: Use of resources in Y1 for WP6. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.7.1 WP7: Objectives

WP7 will integrate the mix-net infrastructure developed in WP4 into the generic open-source LEAP email client as a routing option that preserves the privacy and security of email. In particular, this WP will focus on producing both client and server infrastructure so that routing e-mail through a mix network will prevent various kinds of metadata analysis based on timing information, and will also add padding to prevent attacks on message size. As this open-source e-mail client easily integrates into existing email clients (Outlook, Thunderbird, and others), through use of the integrated VPN/SMTP proxy and an easy-to-use server-side platform, Greenhost can put the mix-net infrastructure of PANORAMIX into the hands of diverse organisations like Mobile Vikings for the widest possible deployment. Objectives:

- *To integrate mix networks into the LEAP open-source client for the routing of email and instant messaging communication.*
- *To determine the initial parameters needed for various levels of user-centric security, privacy, and scalability of the infrastructure developed in WP4 for messaging.*
- *To demonstrate how the generic infrastructure design can be thoroughly integrated and matured within an existing open-source project.*
- *To deploy the generic mix-net in a real-world use-case engaging tens of thousands of users in messaging*

3.7.2 WP7: Progress towards objectives

Requirements were successfully gathered from both developers, systems administrators, and users and fed into WP3 and WP4. Their requirements included detailed user-persona and use-cases (with some input from Mobile Vikings). The requirements outlined the more difficult issues with using SMTP over mix networks, such as spam protection and user churn, that had previously not been considered by previous research in mix nets like Vuvuzela. It was shown that the requirements differed from the requirements needed for e-voting, requiring bi-directional and ideally a dynamic mix net as outlined by KUL. This required new research into

mix networks, as led by UCL. Real data was gathered from email metadata by Greenhost to help parametrize the mix networking components, and detailed threat models created for the privacy and security properties of email. Finally, Greenhost did a large amount of software development work, helping create both key management and encrypted data synchronization for email along, along with a green/red light interface for the VPN and system administration tools. The basic client and server infrastructure is complete, and integration with PANORAMIX should be possible in the second year. This work was successfully captured in D7.1.

3.7.3 WP7: Deviation from objectives

One partner, Mobile Vikings, has left the PANORAMIX Consortium due to being acquired by Medialaan, another Belgian company. Although Mobile Vikings did initially interface well with the consortium and contributed a small amount to the use-cases and requirements as well as attended meetings, after the acquisition the key employees who understood PANORAMIX stopped participating in the project. However, Medialaan (Mobile Vikings) chose to withdraw from the Consortium with the agreement of the PANORAMIX consortium. Therefore, currently WP7 is looking for a new partner with experience in mobile development and with a user-base that can test the mix-net enabled software. Currently, there are several interested companies, including Open Whisper Systems (who develops the encrypted messaging Signal application, with over 1 million users, and also designed the protocol used by WhatsApp for encrypted messaging) as well as the developers of K-9 Mail, the most popular Android client for email with over 5 million downloads.

In addition to issues with Mobile Vikings, there were some difficulties with staffing and administration of the project by Greenhost, but these should be expected of a SME that has not done many EC projects before. In detail, the CEO of Greenhost, Sacha van Geffen, is committed to the project and personally attended the launch meeting, but became too busy to personally write the deliverables. Greenhost also encountered some difficulties in hiring more developers (although it was resolved). In order to correct the situation, Greenhost hired Harry Halpin, one of the original authors of the PANORAMIX proposal, in order to work through the administration, co-ordinate the development effort of PANORAMIX for WP7, and complete the writing of the deliverables. At this point due to the corrective actions, Greenhost has successfully written D7.1 (with some input from Mobile Vikings before leaving the Consortium) and has completed a large amount of development work on both the client and server-side, having also been successful in communicating its use-cases and requirements to WP3 and WP4.

3.7.4 WP7: Beneficiary involvement

UCL led the task to translate the messaging use-cases and requirements into research questions and new technical designs.

UoA helped co-ordinate communication between the partners and provided technical insight.

UT outlined the differences between messaging and e-voting.

KUL took the lead on integrating the use-cases and requirements into WP3.

GH took the lead on editing D7.1, eliciting use-cases and persona, privacy-preserving data collection, and open source software development.

MV gave input into use-cases and persona for mobile messaging.

Table 3.7 shows the use of resources for WP7 in Y1.

Partner	Work Package 7		
	PMs completed in Y1		Total PMs
UEDIN	0	✓	2
UCL	5	✓	24
UT	0.5	✓	2
KU Leuven	3.4	✓	10
GRNET	0	✓	0
SAP SE	0	✓	0
Greenhost	26	✓	84
Mobile Vikings	1.5	×	32
UoA	0	✓	4
Total	**36.4**	✓	**158**

Table 3.7: Use of resources in Y1 for WP7. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y1, a yellow "✓" suggests that the partner allocated a different percentage but this is consistent with the grant agreement use of resources, while a red "X" signifies a deviation (which is explained in the relevant section: "Deviation from objectives."

3.7.5 WP7: Documents and deliverables produced

- D7.1: Applying Mix Nets to Email Document (Editor: GH) [Due: M9] This report presents the use-case and requirements, based on empirical data, of the mix networking infrastructure, with a focus on usability, a mathematical analysis of the privacy set, and threat models.

Deliverable D7.1 was delivered on time (08/06/2016) and accepted by the reviewers.

4. Critical implementation risks and mitigation actions

4.1 First year implementation risks

In this section we refer to the relevant implementation risks as identified in Section 1.3.5 of the grant agreement and how these risks were dealt with in the course of the project. From the 17 risks that were identified only two are relevant for the current stage of the project and are described below.

R1 "Consortium management: partners fail to communicate efficiently, disclose information or provide deliverables." Some minor communication problems were encountered in the implementation of WP7. There are two industry partners involved in this work package, Greenhost and Mobile Vikings. These were mitigated successfully as detailed in the next section. Team forming problems were faced by partner UoA. Specifically, the team of partner UoA consisted of researcher N. Alexopoulos who decided to leave the consortium partner UoA and continue to pursue a Ph.D. on a different topic at a university outside Greece, as well as post-doctoral researcher A. Angelakis, who while being on a testing period working for the project became ill and stopped participating in the project activities.

R13 "Organizational obstacles to exploitation: The result of an EU innovation action is risky and not easily planned for by product organizations. Hence they may be reluctant in uptake." Originally this risk was considered high for consortium partner SAP, however the acquisition of project partner Mobile Vikings by Medialaan in Belgium lead to a change in the general strategy of Mobile Vikings and a need to re-evaluate the viability of their original exploitation plan.

4.2 Mitigation actions

In this section we describe the mitigation actions taken by the coordinator to handle the risks that were manifested in the first year.

R1 The coordinator organized teleconference meetings with WP7 leader Sacha Van Geffen and reevaluated his availability. Subsequently, Sacha on behalf of Greenhost appointed Harry Halpin as WP7 leader.

Regarding the UoA team, the coordinator engaged in teleconference communications with researcher Alexopoulos in order to ensure that work is completed even after his departure to his new institution. The researcher committed substantial personal time even after his departure from consortium partner UoA. Furthermore, with the supervision of the coordinator, a new post-doctoral researcher is sought for partner UoA and meanwhile necessary tasks are covered by partner UEdin.

R13 The coordinator organized teleconference meetings with Tatjana Vandenplas and considered various options for possible exploitation activities by Mobile Vikings taking into account that the partner now is part of Medialaan. As a result of these meetings, a new strategy for exploitation was outlined and integrated in deliverable D2.5.

Currently, further steps are being taken as mentioned above in 3.7.3. WP7 is exploring new partner options such as Open Whisper Systems and the developers of K-9 Mail as a replacement for Mobile Vikings.

5. Plan for year 2 of the project

The second year of the project is critical in the sense that the general effort invested in the first year for modeling and understanding the necessary requirements for building a mix-net needs to culminate in a working system. A minimum viable product should be presented by Month 18 and the final integrated system by Month 24. The following milestones are anticipated.

- (MS6) Minimum Viable Product by Month 18.
- (MS7) Complete Model & First Iteration by Month 20.
- (MS8) Integrated Mix-net System by Month 24.

The coordinator anticipates that the consortium will be able to reach the milestones within the planned timeframe. In addition to the above, with the completion of the second year a complete exploitation plan will be produced (D2.6).

Finally, at the time of this writing, the consortium is in active negotiations with potential partners to be included in the consortium in place of partner Mobile Vikings who did a voluntary exit shortly after the end of Y1. We anticipate that early on in Y2, we will have a partner replacing Mobile Vikings become member of the consortium.