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

Y2 Review and Assessment

Deliverable D1.2

December 15, 2017
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Dissemination Level: Public

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2017-06-01	MW (UEDIN)	Initial Draft
0.2	2017-08-02	MW (UEDIN)	Input from partners incorporated
0.3	2017-08-11	PC (UoA)	Review
0.4	2017-08-17	MW (UEDIN)	Revision after review
0.5	2017-08-28	AK (UEDIN)	Final review
1.0	2017-08-31	MW (UEDIN)	Final version and submission to the EC
1.1	2017-11-28	MW (UEDIN)	Revisions due to Y2 review
1.2	2017-12-14	AK (UEDIN)	Final review of revised document
2.0	2017-12-15	MW (UEDIN)	Final version and submission to the EC

Executive Summary

This report, the second of three, encompasses the project activities from September 2016 through to August 2017. 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 two has been in line with the objectives and work plan as specified in the DoA with the exception of a delay in WP4 and WP7 due to the exit of partner Mobile Vikings and the process of induction of a new partner to the consortium that required minor alignments in the DoA. The new partner – the Center for the Cultivation of Technology– was officially accepted into the consortium on the 3rd of April 2017. To address this delay, a five-month extension was requested as an amendment to the grant agreement and approved on 31/07/2017. This report concludes by setting out the directions for the final part of the project.

Contents

1. Introduction

1.1 Purpose of Document

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

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 CCT and Greenhost).

2. Second Year Summary

The second year of the project was critical in the sense that the general effort invested in the first year for modelling and understanding the necessary requirements for building a mix-net culminated in a working system. A minimum viable product was presented by Month 18. The final integrated system is well on its way to completion, due at the end of January 2018.

At the end of Y1, one of the partners, Mobile Vikings, pulled out of the consortium. A new partner was sought to fill the gap created (mainly in WP7) by their departure. A new partner, the Center for the Cultivation of Technology (CCT) was introduced to the consortium and found to be a good fit complementing the team working in WP7. The amendment to the Grant Agreement necessary to formalise the termination of Mobile Vikings and the addition of beneficiary CCT was formally signed on the 3rd of April 2017. CCT is responsible for the integration of the Panoramix mix-net technology into a development branch of a widely used open source mobile messaging application (K-9 Mail) and will be performing user testing as part of WP7.

Inevitably, the change of partner resulted in some time loss, roughly 7-8 months. Therefore in July 2017, PANORAMIX applied for a 5-month extension to the project which was granted on the 31st of July 2017. It was felt that the quality of the final outcome of PANORAMIX would be of greater value to the European Community if the project was extended. A result of the extension (relevant to this Y2 report) is that two M24 deliverables (D4.3 Integrated System and D7.2 Open-source code of integrated system for desktops) have been moved to M29.

All other deliverables have been submitted according to the original schedule.

2.1 Work Performed — Main Results Achieved So Far

Highlights of the work carried out in Year 2 can be categorised as follows:

- Fifteen papers reporting on PANORAMIX research were published at top-tier cryptography and security conferences during Y2. This is more than double the key performance indicator target that was originally aimed for.

  PANORAMIX was very well represented at the USENIX Security Symposium in Vancouver, Canada one of the top-level international conferences in security. Advances on anonymous communication primitives were presented with two of the three papers in the Privacy & Anonymity Systems track authored by PANORAMIX members.

  The bulk of the research carried out in WP3 up until M20 is described in D3.2.

- PANORAMIX successfully demonstrated its core technology at the 10th International Conference on Computers, Privacy & Data Protection (CPDP) in Brussels on the 26th of January 2017. 21 members of PANORAMIX attended the conference.

  The demo consisted of an educational video —shown on a large TV screen-– explaining the overarching idea of PANORAMIX and its applications. In addition, the Minimum Viable Product (MVP) (D4.2, D5.2) was demonstrated in the form of a private anonymized chat room developed by project partner GRNET. Conference participants were able to see live

how messages can be broadcast anonymously, without allowing an eavesdropper or even legitimate users to figure out which user sent which message.

- Deliverable D6.1 shows how PANORAMIX is being applied in the setting of the statistics use-case and its particular requirements.

- In Deliverable D2.6 "Complete Exploitation Plan", the second version of the exploitation plan for PANORAMIX is presented. It includes detailed exploitation plans for each partner and the joint exploitation plan around the engaging in a token-based ecosystem for privacy-enhancing technologies.

- For WP7, considerable effort was expended to design the specifications for the PANORAMIX decryption mix network: `https://github.com/Katzenpost/docs`.

Beyond the above, progress on most tasks of the project has been made as planned. Figure 2.1 shows the portion of the GANTT chart that corresponds to the project's first two years and shows the percentage of time that has passed (of the original time allocated) for each task, taking into account the five-month extension. This figure gives an impression of the tasks that have been completed in Y1 and Y2, as well as which ones will be the focus for the remainder of the PANORAMIX project's duration.

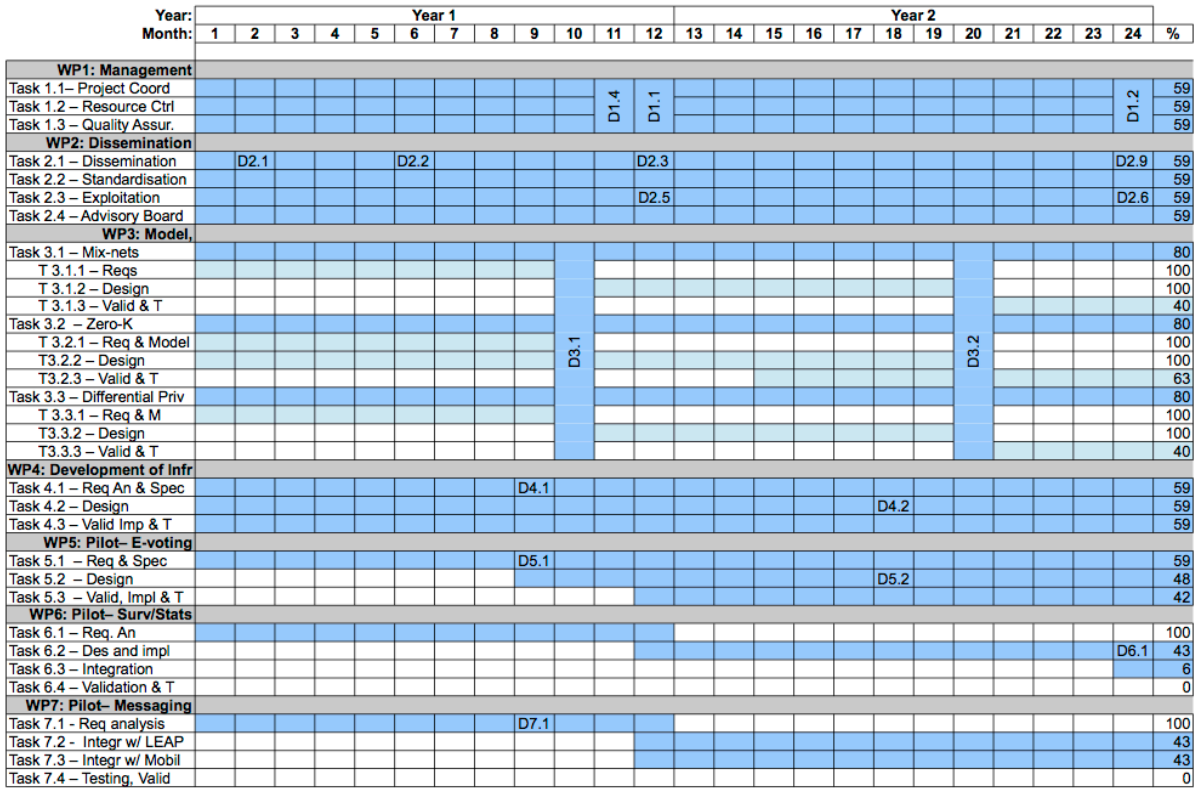

Figure 2.1: *GANTT chart for Y1 and Y2 of the project including the percentage of time that has passed for each task.*

2.2 Milestones Reached

In the second year of the project, the following milestones were reached (milestones MS1-MS5 were achieved in Y1, see Deliverable D1.1):

- (MS6) Minimum viable product
- (MS7) Complete model and first iteration report

3. Second Year Achievements & 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

This section first describes the steps taken as a result of the first periodic review and then goes into more detail how the progress towards objectives was achieved for WP1 in Y2. There were five main recommendations to the consortium after the first periodic review that were taken on board in Y2. In short the recommendations concerned the following areas:

1. Documentation (template, quality control).
2. Public profile and website.
3. Requirements (D4.1).
4. Review and resubmission of deliverables.
5. Ethics.

The recommendations were addressed as follows. A project manager was attracted after the conclusion of Y1 to assist in the day-to-day managing of PANORAMIX. One of the roles of the project manager is Quality Assurance Coordinator (QAC). A Quality Assurance Plan (QAP) was designed by the QAC as a direct result of Recommendation 1. The QAP has been implemented successfully and all the deliverables in Y2 have been produced keeping the QAP time-line as well as ensuring consortium internal reviewing of all deliverables. The deliverable template was adjusted to include a version history, which ensures it is clear who is responsible for editing the deliverable as well as the consortium internal review process.

The PANORAMIX web-site has been amended to include EU funding information, as well as more extensive information about the project including partner's roles in the project. The Publications tab now has a sub tab for public deliverables. Contact information for the project coordinator and the project manager have been provided. A Twitter account has been created (@PanoramixH2020) and the twitter feed is visible in the footer of all PANORAMIX web pages. Throughout the year regular blog updates have appeared on the website and a video explaining the core technology of PANORAMIX has been uploaded. Detailed analytics of both the website and twitter account are given in D2.9.

Regarding the recommendations on Requirements and Ethics, both these were addressed in the revised version of D4.1. Review and resubmission of the rejected deliverables was overseen by the Coordinator and the QAC ensuring the quality of resubmitted deliverables was greatly improved. All rejected deliverables were resubmitted by October 31, 2016 and formally approved by January 24, 2017.

Our progress in WP1 was centred around the three tasks that make up the bulk of the activity in the WP namely Task 1.1: Project coordination and communication, Task 1.2: Resource control and Task 1.3: Quality Assurance.

In addition to sharing regular project information with the project officer, the coordinator liaised with the project officer regarding two separate amendments to the Grant Agreement. First, the coordinator, in collaboration with Greenhost and CCT, prepared the amendment for CCT's accession to the consortium as well as the official termination of Mobile Vikings' involvement with PANORAMIX. Second, a no-cost extension to the project was requested justified by the delay introduced by the changing of partner and supported by a final dissemination activity at CPDP in January 2019.

The OpenProject system introduced in Y1, is still being used by the whole consortium for version control of deliverables, management of meetings including minutes recording and dissemination. Monthly project meetings are conducted via teleconference on the last Wednesday of the month. The Work Package Leader Board (WPLB) and the Project Steering Committee are present at these meetings as well as any consortium members that are available to attend.

The January WPLB meeting (01/24/2017) coincided with our face-to-face meeting in Brussels prior to the CPDP conference. Six members of our External Advisory Board were able to attend (Bart Preneel, Gus Hosein, Jacques Bus, Marit Hansen, Omer Tene & Sven Heiberg) After the periodic report for Period #1 was accepted by the EC and the related interim payment was received the transfer of budget to the partners was taken care of by the coordinator (Task 1.2). Ongoing monitoring of the use of resources within the consortium is being performed. To ensure effective quality assurance (Task 1.3) a project manager (QAC) joined in October 2016.

3.1.3 WP1: Beneficiary Involvement

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

Table 3.1 shows the use of resources for WP1 in Y2.

Partner	Work Package 1				
	PMs completed in Y1		PMs completed in Y2		Total PMs
UEDIN	2.72	✓	5	✓+	7.2
UCL	1.08	✓	1.5	✓	5.4
UT	0	✓	0	✓	0
KU Leuven	0	✓	0	✓	0
GRNET	0	✓	0	✓	0
SAP SE	0	✓	0	✓	0
Greenhost	0	✓	0	✓	0
CCT (MV inY1)	0	✓	0	✓	0
UoA	0	✗	0	✗	14
Total	**3.8**	✓	**6.5**	✓	**26.6**

Table 3.1: Use of resources in Y2 for WP1. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.1.4 WP1: Deviation from Objectives

As mentioned in D1.1, there were some difficulties in coordination and quality assurance during Y1 due to the limited availability of Sacha van Geffen (Greenhost). The task of quality assurance control fell back to the coordinator and a project manager (Mirjam Wester) was attracted to assist in the day to day coordination and as QAC. This also explains the extra PMs indicated for UEDIN. Extra resources needed at UEDIN to ensure all tasks in WP1 are executed well will be taken from the underspent budget of partner UoA.

3.1.5 WP1: Documents and Deliverables Produced

- D1.2 Y2 Review and Assessment (Editor: UEDIN) [M24] The current document.

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

Task 2.1 – Dissemination and Networking. The Y2 dissemination results are reported in Deliverable D2.9, all targets for dissemination have been met, and most quite substantially exceeded. A few highlights from D2.9 are:

- Fifteen papers were presented and published at top-tier cryptography and security conferences. In addition to this, four journal papers were published. Naturally, the main group of people reached with this type of dissemination is the research and scientific community.
- Awareness in industry was raised through the various industry events PANORAMIX contributed to industry and developer oriented forums such as Black Hat, Def Con, Tor developer meetings, etc.
- We also engaged with the general public through presentations at e.g., the Edinburgh Science Festival, an article in Forbes magazine, and an Imec Workshop amongst others.

The PANORAMIX webpages are kept up to date with regular updates to the publications and blogs describing our news, successes and advertising key dissemination activities. In addition to the webpages, there is now also the PANORAMIX twitter feed, (@PanoramixH2020) which is used as another way of engaging the wider public with PANORAMIX.

Task 2.2 – Standardisation: further steps were taken regarding W3C and IETF (see also D2.6). In terms of standardization, KUL, UCL, and CCT have begun collaborating on a group of specifications that can serve for independent implementation of the mix-net messaging use-case, based on decryption mix-nets and the Sphinx packet format. A pre-standardization mailing list has been set-up to co-ordinate the development between implementers of mix networking for messaging; the mixnetworking mailing list is `mixnetworks@lists.mixnetworks.org`.

Task 2.3 – Exploitation: Deliverable D2.6 gives the second version of the exploitation plan for PANORAMIX. It gives a revised version of the joint exploitation objectives as well as updates of the exploitation activities carried out by all partners in PANORAMIX during Y2. The exploitation plans for CCT have been included in place of those that were previously there for Mobile Vikings. D2.6 also includes more details on the joint exploitation plan and the timeline in the third-year for the strengthening and long-term sustainability of PANORAMIX after the end of EC funding. Business models for each of the three use-cases have been set out.

The EAB, as part of Task 2.4, were invited to join us in our face-to-face meeting in Brussels in January 2017. Six of eight of the members were able to attend. This gave us the opportunity to present the ongoing progress in PANORAMIX and specifically the Minimum Viable Product which was due to be shown at the CPDP conference in the next few days and receive the EAB's expert advice and feedback. The EAB were the first to see the PANORAMIX video which illustrates the core PANORAMIX technology in a really engaging and clear manner.

3.2.3 WP2: Beneficiary Involvement

Role of the partners (see also Table 3.2):

UEDIN (lead) led this work package (Tasks 2.1 & 2.4)

ALL all partners contributed to the tasks as detailed above and specifically by participating in international conferences, promoting standardization efforts and publishing their work (Tasks 2.1 & 2.2)

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

KUL participated also on standardization efforts (specification writing and reviews).

GRNET managed the exploitation report and coordinated all partners regarding their exploitation strategies and the business models for market adoption (Task 2.3).

Table 3.2 shows the use of resources for WP2 in Y2.

Partner	Work Package 2				
	PMs completed in Y1		PMs completed in Y2		Total PMs
UEDIN	0.48	✓	1.4	✓	2
UCL	1.3	✓	1.8	✓	6
UT	1.6	✓	2.8	✓	6
KU Leuven	1.5	✓	2.6	✓	5
GRNET	0	✓	1.6	✓	16
SAP SE	4.1	✓	2.3	✓	7
Greenhost	2	✓	2	✓	6
CCT (MV inY1)	4.1	✓+	0.5	✓	6
UoA	0	✗	0	✗	4
Total	**15.08**	✓	**15**	✓	**58**

Table 3.2: Use of resources in Y2 for WP2. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.2.4 WP2: Deviation from Objectives

The partner responsible for editing D2.9 moved from KUL to UEDIN, as it fit more neatly with the role of the project manager. The underspending of resources by UoA in this WP is offset by more resources being used by UEDIN to cover all necessary tasks.

3.2.5 WP2: Documents and Deliverables Produced

- D2.6 – Complete Exploitation Plan (Editor: GRNET) [Due: M24] Includes updates to exploitation activities already performed and includes definition of business models for market adoption of results of the project.
- D2.9 - Dissemination Report II (Editor: UEDIN) [Due:M24] Dissemination activities performed in Y2.

Both WP2 deliverables were submitted at M24.

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 system's cost of the mix-net.*

3.3.2 WP3: Progress towards Objectives

The bulk of the WP3 work undertaken in PANORAMIX months 12 to 24 were delivered in D3.2 in three parts. First an efficient Non-Interactive Zero Knowledge proof for correct shuffling was designed and evaluated. This relates to Task 3.2, on robust shuffling protocols to support

elections. The work carried out at UT has led to more efficient shuffles designed by leveraging pairing-based cryptography and more secure SNARKs were achieved by studying the security requirements around the common reference string needed for SNARKs and how to make those less prone to adversary manipulation.

Secondly, as part of Task 3.1 (supporting message based mix networks and WP7) we undertook the design of Loopix [PHE+17], a modern low-latency mix network; and also the design of a software/hardware based architecture that preserves the privacy of the mix-net decryption keys even under hardware compromises. The MCMix anonymity system (UEDIN) developed a protocol using multiparty computation (MPC) to establish anonymous channels between senders and recipients of messages efficiently [AKTZ17]. Additionally, the use of multi-party computation was explored to implement secure shuffling, and a concrete system that operates on that basis. We also considered how receipt and challenge based mechanisms may be used to improve the robustness of message based mix-nets under active attacks [MCS+17].

Thirdly, as part of Task 3.3 (on measure of anonymity and differential privacy) we researched modern security definitions for anonymity systems, based on cryptographic indistinguishability notions. This resulted in the AnNotify notification system (UCL): A protocol for privacy-preserving publish-subscribe, levering mix-nets to gain greater efficiency [PHG+17]. Work at SAP focussed on differentially private stream analytics. Traditional privacy preserving statistics are for single release settings, in this work this was extended to streaming analytics [BBK17].

In addition to all the research that was carried out in WP3, serving the needs of the use-cases is evidenced by three main streams of support: shuffles, decryption mix-nets and differential privacy. The research on **shuffles** was implemented at GRNET during a visit from UT in which work was carried out to implement the secure shuffle techniques from Asiacrypt'16 [FLZ16] and Asiacrypt'17 [ABLZ17] in Python. A visit from UCL to GRNET was used to present and integrate features from the Loopix design into the Panoramix **decryption mix-net** framework. Work streams at KUL and SAP involved empirical performance evaluation of the current Panoramix mix-net. Effort was made to transfer the AWARE **differential private** statistics designs into exploitation in WP6.

Overall, at the technical level, the consortium did a decisive step in bridging the gap between theory and practice in mix-nets. Loopix and MCMix are prototype systems that demonstrate how mix-nets can be implemented securely and the zero-knowledge shuffle and privacy preserving statistics protocols we proposed are the current state of the art in performance and security. Software repositories for both systems are available; for the Loopix anonymity system: `https://github.com/UCL-InfoSec/loopix` and for MCMix code: `https://github.com/druid/mcmix-benchmark`.

3.3.3 WP3: Beneficiary Involvement

The work carried out by each partner has closely followed the original plan, see also Table 3.3:

UCL (lead) coordinated the WP3, and worked on robustness against hardware compromises, anonymity measures (Tasks 3.1 and 3.3).

KUL The Loopix anonymity system is a collaboration between UCL and KUL (Task 3.1).

UEDIN Produced the MCMix anonymity system (Task 3.1).

UT provided the work on provable shuffles (Task 3.2).

UEDIN/UoA is pursuing the work on secret sharing based shuffles (Task 3.1).

SAP evaluated the use of differential privacy in the local model where data is anonymized at the data source, before collection, in conjunction with the Panoramix mix network. They further continued research towards the use of differential privacy for text and log data analysis (Task 3.3).

Table 3.3 shows the use of resources for WP3 in Y2.

Partner	Work Package 3		
	PMs completed in Y1	PMs completed in Y2	Total PMs
UEDIN	0.96 ✓	8 ✓	20
UCL	7.62 ✓	12 ✓	36
UT	18.5 ✓	40 ✓+	42
KU Leuven	11.7 ✓	9 ✓	30
GRNET	0 ✓	0 ✓	0
SAP SE	6.06 ✓	5 ✓	12
Greenhost	0 ✓	0 ✓	0
CCT (MV inY1)	0 ✓	0 ✓	0
UoA	3.5 ✓	3 ✓	12
Total	**48.34** ✓	**77** ✓+	**152**

Table 3.3: Use of resources in Y2 for WP3. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, a green "$\checkmark^{+}$" 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.3.4 WP3: Deviation from Objectives

Everything was executed largely according to plan. The high number of PMs for academic partner UT (see Table 3.3) is due to a different make up of the local workforce than initially envisioned. The financing remains the same, but instead of two post-docs to do the research, one post-doc, three phd students and a master student have been carrying out the work, which explains the increase in PMs.

3.3.5 WP3: Documents and Deliverables Produced

- D3.2: Design, modelling and analysis (Editor: UCL) [Due: M20] First iteration of a NIZK shuffle proof. Describes the shuffle protocol that may be used in implementation within WP5; Integrates robustness into efficient mix-net designs and decryption mixes; proposes robust definitions of mix-nets as differentially private mechanisms.

Deliverable D3.2 was delivered on time (30/4/2017).

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

In order to support the realization of the use-cases, we provide the implementation of a state of the art mix network along with a wizard to set it up and an API which allows each use case to implement their requirements (Task 4.1). The mix network design (Task 4.2) comes from research published by WP3, whereas the API has been validated by WP5, WP6 and WP7 to ensure it is possible to build the different use-cases on top of the implemented software package.

With regards to the scalability of the system, the mix network technology is already scalable by default; however, we still needed to take care of the configuration and deployment phases, which we designed to be both easy and practical for large deployments.

The Minimum Viable Product delivered in D4.2 allowed partners to agree on a stable API, as well as on the requirements that constitute the core of the Panoramix platform. Their implementation provided a basic library that WP5, 6 and 7 can already make use of, e.g. by measurement the performance of the different mix networks included, or by developing the software architecture that accommodates with the public API. Code repository of the Panoramix Minimum Viable Product (MVP): `https://github.com/grnet/panoramix`.

In addition to the MVP, the mixnet specification for WP7 facilitated conversations between WP4 and WP7 teams, setting up the architecture that will power the email service and solving specific problems to it such as the need for bounce messages. The effort will be at the heart of WP7 adoption of Panoramix, making the framework directly used by the K-9 email client and the LEAP ecosystem.

The current prototype has been publicly demonstrated and we are now ready to improve the performance and the ease of configuration of the system. The introduction of a practical PKI and the implementation of new requirements coming from WP3 will complete the system and provide all the functionality required by the use-cases (Task 4.3).

3.4.3 WP4: Beneficiary Involvement

This work package requires participation from most partners (see also Table 3.4). A coarse breakdown follows:

Academia UoA, UCL, UEDIN, UT and KUL helped to specify the requirements (Task 4.1) and provided design recommendations to the implementers (Task 4.2).

GRNET implemented most of the software package (Task 4.3), crafted its design (Task 4.2), tested the system and validated its API with regards to WP5 (Task 4.3).

UT implemented a specific type of mix network –the subversion-resistant framework for SNARKs introduced in the article "A Subversion-Resistant SNARK" – which was incorporated in the Panoramix package (Task 4.3).

GH validated the API and helped to specify the requirements related to WP7 (Task 4.1).

KUL organized meetings, scheduled internal deliverables and lead the specification of the mix network architecture related to WP7 (Task 4.2).

CCT contributed to the specification of the mix network architecture related to WP7 (Task 4.2).

Table 3.4 shows the use of resources for WP4 in Y2.

Partner	Work Package 4		
	PMs completed in Y1	PMs completed in Y2	Total PMs
UEDIN	0.24 ✓	2.5 ✓	16
UCL	2.62 ✓	3.5 ✓	12
UT	1.6 ✓	3.6 ✓	12.8
KU Leuven	3.1 ✓	3.5 ✓	10
GRNET	16.31 ✓	16.83 ✓	48
SAP SE	0 ✓	0 ✓	0
Greenhost	4 ✓	5 ✓	14
CCT (MV inY1)	3.2 ✓	3 ✓	8
UoA	0 ✗	3 ✓	30
Total	**31.07** ✓	**40.93** ✓	**150.8**

Table 3.4: Use of resources in Y2 for WP4. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.4.4 WP4: Deviation from Objectives

The accession of a new partner CCT, involved the redistribution of tasks based on the new opportunities and capacities that CCT offers, and the mapping of the requirements to the new target application (K-9). Whereas the previous partner, MV, envisioned a mobile client that used email as a way to show an experience close to instant messaging, K-9 is a traditional email client.

On the other hand, the specification of the architecture and the parameters of the mix network underlying WP7 application is a necessary step to make sure the final product is delivers the experience final users expect. We have put a substantial amount of effort into this task, increasing the time needed to achieve WP4 objectives.

3.4.5 WP4: Documents and Deliverables Produced

D4.3 was originally due M24 but has been postponed to M29 as a result of the 5-month extension to the project.

- D4.2: Minimum Viable Product (MVP) (Editor: KUL) [Due: M18] A functional, deployable and demonstrable mix-net service implemented according to results from the other WPs was presented at CPDP 2017 in Brussels.
- D4.3 Integrated System (Editor:KUL) [Due:M29]

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

Continuing the work of the first year of the project, in the second year work focused on implementing a faster mix-net for voting. To recap, the existing system, Zeus, mixes votes with a Sako-Kilian re-encryption mix-net. This is a simple mix-net, that is secure, but not very efficient. Only a few thousand ballots can be handled within an acceptable amount of time (about an hour). The research outcomes of WP3 are being used to improve this resulting in orders of magnitude faster election processing. In particular, GRNET worked with UT to implement their mix-net described in "A Shuffle Argument Secure in the Generic Model" [FLZ16]. This mix-net is much faster than the existing Sako-Kilian mix-net currently used by Zeus, and measurements show that it can handle thousands of cipher texts in minutes.

GRNET and UT worked together in implementing a Python prototype directly from the specification given in the paper. Then, GRNET worked on a faster implementation, based on Cython, which runs the cryptographic primitives in C++ code while providing convenient Python wrappers so that it can interact easily with the rest of the Zeus infrastructure. Python implementation available at: `https://github.com/grnet/ac16`.

More recently, a further improved mix-net, described in "An Efficient Pairing-Based Shuffle Argument" [FLSZ17], has been implemented and incorporated in Zeus. A key component for that was the development of a method for creating, via secure multi-party computation, a Common Reference String (CRS) that is needed as input to the mix-net algorithm. The python implementation of this work is available at `https://github.com/grnet/hat_shuffle`.

The Minimum Viable Product (MVP) was demonstrated at CPDP in the form of a private anonymized chat room developed by GRNET (Task 5.3). Conference participants were able to see live how messages can be broadcast anonymously, without allowing an eavesdropper or even legitimate users to figure out which user sent which message. Concerning the Panoramix framework, work is in progress to ensure that the new mix-net, as well as others, can be used directly on the Panoramix platform. The MVP is available at: `https://github.com/grnet/zeus`.

3.5.3 WP5: Beneficiary Involvement

The work carried out by each partner has closely followed the original plan (see also Table 3.5):

GRNET (lead) coordinated the work carried out in WP5.

UT contributed to the design of the new mix-net (Task 5.2).

UEDIN worked on the analysis of e-voting security (Task 5.1).

Table 3.5 shows the use of resources for WP5 in Y2.

Partner	Work Package 5				
	PMs completed in Y1		PMs completed in Y2		Total PMs
UEDIN	0	✓	1	✓	4
UCL	0	✓	0	✓	0
UT	0.5	✓	6	✓	16
KU Leuven	0	✓	0	✓	0
GRNET	20.62	✓	22.12	✓	62
SAP SE	0	✓	0	✓	0
Greenhost	0	✓	0	✓	0
CCT (MV inY1)	0	✓	0	✓	0
UoA	0	✗	3	✓	14
Total	**21.12**	✓	**32.12**	✓	**96**

Table 3.5: Use of resources in Y2 for WP5. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.5.4 WP5: Deviation from Objectives

There have been no deviations for WP5 in Y2.

3.5.5 WP5: Documents and Deliverables Produced

- D5.2 Minimum Viable Product (GRNET) Demonstrator [Due M18]

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 second year of the project, SAP has been working on the system design and implementation (Task 6.2) of the survey and statistics demonstrator. To this end, we have carried out the following activities:

1. We have selected the specific use case to be demonstrated by our WP6 prototype: We will privately collect and analyze vehicle location data. We collect location data from several (simulated) vehicles, send it over the Panoramix mix-net to provide anonymity, and aggregate the data in a database. The data analyst can then perform a visual analysis of the thus acquired data. A variant of differential privacy called "geo-indistinguishability" will be used locally at the source to protect the location data even against a malicious database or data curator.
2. From the selected use case we have inferred and formulated further concrete requirements for the demonstrator. On one hand, the requirements are based on the actors and the actions they need to perform. On the other hand, we have formulated further requirements related to performance and privacy. Based on the use case and requirements, we have devised the initial design and architecture for the demonstrator, as detailed in our interim report D6.1.

3. We have started the implementation of the prototype of the demonstrator. It currently provides offline functionality (i.e. with static data) where the simulated vehicles send their location to a central server for aggregation in its database. The demonstrator also already supports visualization for the data analyst. As differential privacy mechanism, we have chosen and implemented the planar Laplace mechanism. We have integrated it into the clients (simulated vehicles) to provide geo-indistinguishability for the submitted location data.

We provide a detailed description of the illustrated use case, the requirements, and the initial design in our interim report (D6.1). Completion and integration of our demonstrator with the Panoramix mix-net, as well as the evaluation of the final prototype, will be performed as planned in the final year of the project.

We will use the methods of differential privacy developed in WP3 in order to achieve data confidentiality. Differential privacy is a reliable measure for data privacy. Input randomization as used in many techniques that provide differential privacy can even protect the data against the database and may allow an arbitrary number of queries.

UCL supported the work carried out in WP6 (Task 6.2) by carrying out research dealing with privacy-preserving surveys and statistics. The common thread of this activity is to leverage mix networks as security mechanisms used to engineer further, more complex and useful, privacy primitives. Due to the inherent security properties of mix-nets those security mechanisms cannot be shown to only leak negligible information, and instead we had to innovate in terms of security definitions, to model non-negligible privacy leakage. Thus the definitions of security are inspired and adapted from differential privacy, and enjoy similar properties with respect to side information and composition.

1. The AnNotify system [PHG+17] implements a private publish subscribe system, where users can register their interests with notification providers. Then they can poll and check whether a notification was activated. The association of subscriber to provider remains private, and an adversary cannot tell which events are sought by which users. We also extend the scheme to multiple subscribers and public notifications. The research was done in collaboration with Prof. Herzberg's group at Bar Ilan university.

2. The Mix-ORAM work [TDE17] leverages mix networks to build more efficient, service based, oblivious ram protocols. Those allow users to query specific records they stored in an encrypted form privately – without an adversary knowing which record was accessed. The expensive step in traditional ORAM involves the user "shuffling" and randomizing all records. We propose to use a mix network for this purpose, and show this decreases the client efforts significantly.

3. The s-private PIR [TDG16] suites of protocols propose relaxation of traditional Private Information Retrieval, that are however leaky in terms of privacy – as compared to the unconditionally secure IT-PIR. However, we show a key theorem related to PANORAMIX: such relaxed PIR systems, when composed with an anonymity channel can see their privacy increased arbitrarily. Similar to other works we quantify this using a differentially private metric for anonymity.

3.6.3 WP6: Beneficiary Involvement

SAP selected the specific use case to be demonstrated by the prototype, inferred further use case specific requirements and devised the initial design of the prototype. They also implemented a first offline version of the prototype including location privacy and visual analysis of the results. A detailed description of the illustrated use case, requirements, and the initial design of the demonstrator is given in the interim report (D6.1).

UCL discussed possible improvements to the used location privacy mechanism. Furthermore, UCL performed research towards privacy-preserving surveys and statistics which resulted in the three publications, described above.

Table 3.6 shows the use of resources for WP6 in Y2.

Partner	Work Package 6		
	PMs completed in Y1	PMs completed in Y2	Total PMs
UEDIN	0 ✓	0.5 ✓	4
UCL	3.69 ✓	5 ✓	18
UT	0.5 ✓	0 ✓	4
KU Leuven	0 ✓	0 ✓	0
GRNET	0 ✓	0 ✓	0
SAP SE	7.93 ✓	5.9 ✓	35
Greenhost	0 ✓	0 ✓	0
CCT (MV inY1)	0 ✓	0 ✓	0
UoA	0 ✓	0 ✓	0
Total	**12.03** ✓	**11.4** ✓	**61**

Table 3.6: Use of resources in Y2 for WP6. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.6.4 WP6: Deviation from Objectives

There have been no deviations for WP6 in Y2.

3.6.5 WP6: Documents and Deliverables Produced

- D6.1: Survey/Statistics Interim Report (Editor:SAP) [Due:M24] This report presents the requirements analysis and outlines the initial design used to start the implementation.

Deliverable D6.1 was delivered on time (31/08/2017).

3.7 WP7: Use-case: Messaging

The lead partner for WP7 is Greenhost.

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

The main objectives of the second year were moving from use-cases and requirements to concrete working infrastructure for messaging. In detail, building off the Loopix architecture for dummy traffic from UCL and a six mix-node architecture designed by KUL, Greenhost set-up six distinct hosts to serve as mix-nodes and two "demo" e-mail service providers in order to serve as the backbone of the use of the Panoramix mix network for messaging, with the primary server being in a European jurisdiction (Amsterdam) and CCT contributing server resources in Germany. The entire process for setting up these servers has been extensively documented, allowing new servers to be added to handle increased traffic via load-balancing configurations. Puppet scripts to automate the installation of both generic hardened servers from LEAP have been created that can be easily extended with specialized Panoramix components.

With the aid of implementers from CCT and feedback on deployment by GH, an impressive set of specifications covering the architecture, the packet format (Sphinx), and the mix PKI have been authored to guide implementation of the cryptographic details by the implementation partners in WP7. These specifications specialize the generic infrastructure `https://github.com/Katzenpost/docs`. These specifications are quite mature, and may eventually serve as the basis of standardization at the IETF. Integration with incoming e-mail via particular SMTP headers and out-going email via the use of checking the mix PKI are also underway, allowing Panoramix to be fully integrated into the open-source LEAP architecture and so easily deployed by future secure communication providers. A formal computational proof of the security and privacy properties of the messaging mix network has also been started to allow a principled understanding of the privacy properties mix-net messaging relies on in contrast to other systems for anonymous messaging such as Tor.

3.7.3 WP7: Beneficiary Involvement

GH is leading the overall WP, the writing of D7.2, and deals with server-side deployment considerations as well as the LEAP/Bitmask desktop client work.

UCL is leading the work on the specifications in Task 7.2 and analysing the data-set gathered as part of Task 7.1, contributing their expertise in the Sphinx message packet and the Loopix system in particular.

CCT has just started on PANORAMIX, replacing MV. They are leading the Android work and core contributors the mix-net messaging specifications.

KUL is also actively contributing the messaging specifications and the analysis of the messaging data-set gathered as part of Task 7.1.

UoA is working with UEDIN on the formal analysis of the messaging mix-net use-case.

UEDIN is leading the formal analysis of the security and privacy properties of the mix-net use-case.

Table 3.7 shows the use of resources for WP7 in Y2.

Partner	Work Package 7				
	PMs completed in Y1		PMs completed in Y2		Total PMs
UEDIN	0	✓	1	✓	2
UCL	5	✓	5.5	✓	24
UT	0.5	✓	0	✓	2
KU Leuven	3.4	✓	2.7	✓	10
GRNET	0	✓	0	✓	0
SAP SE	0	✓	0	✓	0
Greenhost	26	✓	29	✓	84
CCT (MV inY1)	1.5	✗	6.2	✓	32
UoA	0	✓	0	✓	4
Total	**36.4**	✓	**44.4**	✓	**158**

Table 3.7: Use of resources in Y2 for WP7. Legend: A green "✓" suggests that the partner allocated approximately 1/3 of the total budget in Y2, 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. Deviations are justified in the relevant section: "Deviation from objectives."

3.7.4 WP7: Deviation from Objectives

There have been a number of deviations from the initial plan. First, the departure of Mobile Vikings from the project caused a major problem insofar as they were tasked to deliver the mobile Android client for messaging using the mix network. However, the new partner CCT was added, although they did not receive funding for new resources on a mobile Android Client until May 2017. This set work back several months, motivating the request for a 5-month extension which has been granted. This will allow for CCT's work on the mobile K-9 client catch up.

Second, work on the Pixelated client also required more work than expected due to scalability issues in the underlying LEAP platform and the withdrawal of some open-source contributors from the Pixelated Desktop client, which should also be addressed by the extension. Lastly, there was more work from UCL and KUL, in conjunction with CCT and with feedback from GH, to adapt the Panoramix architecture to the detailed specifics of the mix networking use-case.

3.7.5 WP7: Documents and Deliverables Produced

D7.2 was originally due M24 but has been postponed to M29 as a result of the 5-month extension to the project.

- D7.2 Open-source code of integrated system for desktops (Editor: GH) [Due: M29] This deliverable is available as code on GitHub with a brief developer guide to the code.

4. Plan for Year 3 of the Project

The third year of the project will be 5 months longer than originally envisioned, the revised end date will be 31/01/2019. During the following few months we will concentrate on ensuring the integrated system is complete, tested, and well-documented incorporating updated requirements and designs from the experience of the MVP. For WP5 this means further incorporation of an improved version of the mix-net into the Zeus infrastructure. In the survey/statistics use-case, experiments are underway testing the mix-nets from the MVP. In WP7, work will focus on ensuring open-source code of integrated system for desktops will be completed. This will allow system administrators to deploy the mix networking infrastructure for email, with clients for desktop and mobile. In all three use-cases, this will be followed by more effort on validation, product implementation and testing.

The following milestones are anticipated:

- (MS8) Integrated Mix-net System by Month 29.
- (MS9) Second Iteration and Security Analysis Report by Month 30.
- (MS10) Final System and User Feedback Analysis by Month 41.

Exploitation and a long-term project sustainability plan for PANORAMIX has been described in D2.6. It includes detailed exploitation plans for each partner and the joint exploitation plan around the engaging in a token-based ecosystem for privacy-enhancing technologies which will be put into place over the course of Year 3. Attention is also given to how the project community will be further developed via a number of measures. These measures will be based on a mixture of *outreach events* that will recruit new developers and companies to the work of the consortium, as well as *developer sprints* to keep the software working and harmonized across the various project partners and stakeholders, and lastly a number of *organizational* events to keep the project internally organized around its goals.

The legal perspective of the PANORAMIX project will be given due consideration in Year 3. The legal analysis will form part of D1.5 (System Misuse/Abuse and Mitigation Strategies) and will include addressing the following research questions:

- To what extent can the deployment of mix-nets contribute to the fulfilment of the requirement of Data Protection by Design ex art. 25 General Data Protection Regulations?
- What are the data protection obligations of an EU-based email service provider when operating a mix-net architecture together with other EU-based email service providers?

Finally, some of the events that PANORAMIX will be engaging with to increase networking across Horizon2020 projects are:

- CPDP 2018: PANORAMIX will be hosting a panel “Anonymous communication infrastructures for the protection of metadata”.

- H2020 Project Clustering Workshop in Athens, organised be ReCRED (`recred.eu`). 15 H2020 projects will meet to present their respective projects, to discuss project outcomes and problems faced during the project's lifespan as well as discover opportunities for collaboration.

Bibliography

[ABLZ17] Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michal Zajac. A subversion-resistant SNARK. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2017.

[AKTZ17] Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, and Thomas Zacharias. MCMix: Anonymous messaging via secure multiparty computation. In Kirda and Ristenpart [KR17], pages 1217–1234.

[BBK17] Jonas Böhler, Daniel Bernau, and Florian Kerschbaum. Privacy-preserving outlier detection for data streams. In Giovanni Livraga and Sencun Zhu, editors, *Data and Applications Security and Privacy XXXI - 31st Annual IFIP WG 11.3 Conference, DBSec 2017, Philadelphia, PA, USA, July 19-21, 2017, Proceedings*, volume 10359 of *Lecture Notes in Computer Science*, pages 225–238. Springer, 2017.

[FLSZ17] Prastudy Fauzi, Helger Lipmaa, Janno Siim, and Michal Zajac. An efficient pairing-based shuffle argument. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 97–127. Springer, 2017.

[FLZ16] Prastudy Fauzi, Helger Lipmaa, and Michał Zając. A shuffle argument secure in the generic model. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 841–872, 2016.

[KR17] Engin Kirda and Thomas Ristenpart, editors. *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*. USENIX Association, 2017.

[MCS+17] Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec, and George Danezis. A touch of evil: High-assurance cryptographic hardware from untrusted components. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1583–1600. ACM, 2017.

[PHE+17] Ania M. Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The Loopix anonymity system. In Kirda and Ristenpart [KR17], pages 1199–1216.

[PHG+17] Ania M. Piotrowska, Jamie Hayes, Nethanel Gelernter, George Danezis, and Amir Herzberg. Annotify: A private notification service. In Thuraisingham and Lee [TL17], pages 5–15.

[TDE17] Raphael R. Toledo, George Danezis, and Isao Echizen. Mix-oram: Using delegated shuffles. In Thuraisingham and Lee [TL17], pages 51–61.

[TDG16] Raphael R. Toledo, George Danezis, and Ian Goldberg. Lower-cost epsilon-private information retrieval. *CoRR*, abs/1604.00223, 2016.

[TL17] Bhavani M. Thuraisingham and Adam J. Lee, editors. *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society, Dallas, TX, USA, October 30 - November 3, 2017*. ACM, 2017.