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

Final Review and Assessment

Deliverable D1.3

May 2, 2019
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	2018-08-28	MW (UEDIN)	Initial Draft
0.2	2019-01-23	MW (UEDIN)	Input from all partners incorporated
0.3	2019-01-26	AK (UEDIN)	Editorial Pass
1.0	2019-01-31	MW (UEDIN)	Final version submitted to the EC
1.1	2019-04-10	MW (UEDIN)	Amendments due to Final Review
1.2	2019-04-17	AK (UEDIN)	Final pass

Executive Summary

This report, the last of three, encompasses the project activities from September 2017 through to January 2019. It evaluates the project outputs as a whole as well as the achievements and results per work package compared against the description of the action (DoA) in more detail. Progress in the final year has been in line with the objectives and work plan as specified in the DoA.

Contents

1. Introduction

1.1 Purpose of Document

The objective of this final review and assessment deliverable is to provide an overview of the project activities in the final year of the project.[1]

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).

[1] We refer to the final period as a year, although strictly speaking it covers 17 months due to the 5-month extension that was approved in July 2017.

2. Final Year Summary

In this summary, we describe the final year of the project and how we have delivered the main goals and objectives of PANORAMIX. Recall that the main idea of PANORAMIX is to provide privacy via mix-nets. Mix-nets, short for mixing networks, are networks of servers that receive messages from multiple senders, shuffle them, and then send them to their final destination. As we look back on the original goals of Panoramix, we can conclude that at the end of the project we have succeeded in achieving both major goals.

- First of all, we have designed and delivered a production implementation of a secure mix-net system that is freely available, fully documented and interoperable.
- Secondly, the three use-cases have demonstrated the use of mix-nets in e-voting, big data (statistics) and private messaging (e-mail).

In addition to the two main goals mentioned above, one of the big goals in PANORAMIX was to create a community around the PANORAMIX system that would take over the maintenance of the software for years to follow the end of the project. We detail how these objectives have been achieved below.

Objective 1: Building a Mix-Net Infrastructure for Europe The PANORAMIX project has created a European mix-network open-source codebase and infrastructure that has been used by the three high-value applications during the project course and will extend beyond the project's duration. The system has evolved towards an easy to use and fully featured product that third parties with different aims can easily use.[1] Full functionality and improved maintainability have closed the gap between the integrated system delivered in D4.3 and the final system. All three use cases have been able to use it to accomplish their goals, and third parties are now able to leverage the same infrastructure to provide privacy-preserving communications based on mix networks. Thanks to the intensive software testing of the software, the code quality has been improved to reach a production ready level, and future maintenance has become easier thanks to the automated testing suite integrated in the system. Applications that are using the Panoramix codebase and infrastructure include the following, reaching our stated KPI target of 5-10 applications.

- Zeus e-voting
- SAP - Anonymized data collection application
- Katzenpost - Android mobile app for anonymised messaging
- *mailproxy* - cross-e-mail client tool
- Libbitcoin Dtek Wallet - integration of cryptocurrency wallet with Panoramix mix-net

[1] This is actually already taking place with e.g., the implementation performed by Google's Deepmind team of our mix-net technology, see `https://github.com/deepmind/loopix-messaging`. Moreover, the lighting network adopted techniques related to and influenced by PANORAMIX research, namely Sphinx extensions and HORNET ideas: `https://github.com/lightningnetwork/lightning-onion`.

- MCMix app for messaging via secure multiparty computation

At the same time, the Nym spin-off of the Panoramix project is building a decentralized authentication and payment protocol which will enable developers to build their own sustainable privacy-enhanced services without relying on the surveillance of users.

The success and continuation of PANORAMIX is further supported by the funding that has already been received by project partners for continuing the work. Examples include the H2020 project PRIVILEDGE (UT and UEDIN) focusing on privacy-enhancing cryptography in distributed ledgers and the Samsung NEXT Stack Zero Grant[2] (CCT) focusing on anonymous communications. Last but not least, Nym, the spin-off company of the project launched in December 2019 with the objective to effectively productise privacy-enhancing technologies such as anonymous communications has received significant venture capital investment.[3]

Objective 2: Mix-Nets for Private E-voting As a result of the collaboration in PANORAMIX, GRNET was able to evolve the e-voting platform such that large scale elections with hundreds of thousands, even millions of voters participating are possible achieving our stated KPI target. D5.4 describes the testbeds and evaluation that show this result. Thanks to the development performed in PANORAMIX, the Zeus e-voting system has the ability to process as many as 1M votes with enhanced privacy and has already been deployed in numerous election procedures as of the writing of this report, cf. D5.4. It is worth noting the high turnover that was achieved in Zeus elections: the mean is 80% and the median is 85% which is significant for the type of elections the system is used for. Overall, as improvements to Zeus have been carried over from work in PANORAMIX since the beginning of the project, the number of elections held with Zeus in this period is 339. Furthermore, the Zeus app showcases how different verifiable mix-nets can be used: Verificatum, Hat-Shuffle and Sphinx.

Objective 3: Mix-Nets for Privacy-aware Cloud Data-Handling In D6.2, we show, by means of the taxi trip data and location information, that we have achieved our KPI for objective 3 to support private gathering of data to compile real time traffic maps or other smart city big data for about *1M-5M updates daily*. Tests carried out by SAP measuring the mix-net's throughput and latency performance showed that a mix-net can be run with a throughput of 20 messages per second, which is 1.7M per day, on an ordinary developer laptop. Migrating to a dedicated server allowed continuous operation of the mix-net with over 5M messages up to 10M messages per day. Furthermore, we show a sweet spot between utility and privacy can be achieved, and that both anonymization strategies (mix-nets and differential privacy) make a valuable contribution by complementary strengths.

Objective 4: Mix-Nets for Privacy-preserving Messaging At the end of Y1, Mobile Vikings one of the commercial partners in the consortium formally terminated their involvement. To mitigate the loss as much as possible, the Center for the Cultivation of Technology (CCT) was invited to join the consortium. The plan was to substitute MV's large user-base with an open-source development project (K-9 Mail) with a substantial user-base in addition to the user-base at Greenhost. Unfortunately, the roll-out of mix-nets for messaging to both user-bases was not possible. Dependencies on an independent platform (LEAP) –which did not reach maturity– prevented roll out to the GH user-base, and policy changes to the Google Play channel meant publishing to the K-9 Mail beta channel was impossible.

Although the number of users for messaging has not reached tens of thousands yet, thus not reaching the respective KPI target by the end of the project, we are confident we will be able achieve these objectives post-project through continued support at both Greenhost and CCT as well as through the new spin-off NYM. User testing has taken place and is described in D7.3. Although the mix-net performance currently does not reach less than 5s for messaging, it is within the user expectations as revealed by the feedback we obtained.

[2] See `https://samsungnext.com/whats-next/introducing-the-samsung-next-stack-zero-grant/`

[3] See `https://www.coindesk.com/this-binance-backed-crypto-startup-wants-to-anonymize-everything`.

2.1 Key Performance Indicators (KPI)

Table 2.1 lists the KPI as envisioned in the Grant Agreement DoA (p 24).

	Performance Dimension	**KPI**	**Target**	**Objective**
1	Increase uptake of mix-networking for the preservation and understanding of end-user Data Protection rights.	Number of end-users using PANORAMIX mix networking across all applications	300,000	Objective 1
2	Create an eco-system of Data Protection-respecting privacy enhanced applications throughout Europe.	Number of applications using PANORAMIX mix networking using the API	5-10	Objective 1
3	Have privacy-preserving e-voting become the norm throughout Europe.	Number of elections held using GRNET's PANORAMIX-enabled e-voting solution.	500	Objective 2
4	Have large scale e-voting platform in place.	Number of voters that may be supported in elections.	1,000,000	Objective 2
5	Determine if improved privacy increases participation in elections via e-voting.	Average voter turnout in PANORAMIX-enabled e-voting solution.	70%	Objective 2
6	Support privacy-preserving data collection at the scale of a major cloud provider.	Number of data generation events per day	1,000,000 to 5,000,000	Objective 3
7	Increase number of end-users that use mix-networks to preserve their privacy for messaging in email and mobile.	Number of users of LEAP client software for GH, CCT, and other providers.	20,000 for GH & 225,000 for CCT (via K9-Mail)	Objective 4
8	Increase the projected speed of mix-networking for e-mail and mobile messaging.	Time for typical message (without attachment) delivery using mix network.	Under 5s for messaging	Objective 4

Table 2.1: Expected impacts using Key Performance Indicators (KPI) for each objective with a quantified target. Taken from Grant Agreement DoA – p24. (Note there is a difference between the tables on p24 (DoA) and p30 (DoA). The table on p30 shows Actions planned to achieve the KPIs, not the actual KPIs.)

Going through each of the KPI sequentially we can state the following about the KPI targets:

1. We reached approximately 80,000 end-users, falling short of the target of 300,000 end-users using PANORAMIX mix networking across all applications. The reason we did not achieve this ambitious KPI was because the users that were envisioned for the messaging use case have not yet been fully engaged (a short explanation is given below, with more detail in Section 3.7.4).

2. Six applications use the PANORAMIX API to date: Zeus, SAP data collection, Katzenpost Mobile app, Mailproxy, Libbitcoin Dtek Wallet and MCMix. In addition to this, Google's Deepmind and the Lightning Network have leveraged the mix-net technology provided by PANORAMIX.

3. During the PANORAMIX project, 339 elections have been held using Zeus.

4. PANORAMIX has put in place a large scale e-voting platform, and now more that 1M voters can be supported in elections.

5. Furthermore, a great success has been reaching average voter turnout of > 80. This exceeds the ambitious goal to increase the participation in elections by e-voting about 70%.

6. More than 5M data generation events per day are possible,

7. One of the KPIs set for objective 4, was not reached. Instead of being able to engage with 20,000 users for GH and 225,000 users vis K9-mail, only 100 users were reached. This was due to various complications in rolling out messaging to the two user groups. The LEAP infrastructure did not get to a sufficient state of maturity to deploy to Greenhost end-users, which prevented a general roll-out of the mix-net to Greenhost end-users. Google Play policy changes prevented publishing the mix-net enabled version of K-9 Mail via the beta channel.

8. The original goal was to get down to 5 seconds for messaging. Currently, messages take typically 30 seconds to arrive through the Panoramix mix-net, with an additional 30 seconds on average to retrieve key material on the first message. However, beta-testing of the alternative *mailproxy* and Katzenpost application showed that for e-mail, 30 seconds to a minute delay was acceptable. Also, for messaging applications, delays up to 30 seconds are often acceptable. Therefore, although reaching very low latencies for messages such as 5 seconds was not reached and so is an objective for future research, the current delivery times of the Panoramix mix-net are capable of supporting the messaging and e-mail use-case for the majority of users.

2.2 Work Performed — Main Results in Y3

Highlights of the work carried out in the final period (September 2017- January 2019) can be categorised as follows:

- Seventeen papers were accepted for publication at a wide range of scientific conferences in addition to three journal papers. This clearly illustrates the academic research output in PANORAMIX has continued to be of the highest standard.

  - The anonymous communication formal analysis work developed by UCL, UEDIN/UoA was published in the top security and cryptography conferences, IEEE Security and Privacy 2018 and Asiacrypt 2018.

  - The CRS verification protocol and techniques that provides privacy of NIZK arguments in case of maliciously created CRS was presented at Asiacrypt 2017 and was subsequently invited to the Journal of Cryptology.

- In addition to a number of dissemination activities jointly with other H2020 projects highlights for the last year having PANORAMIX accepted to present at CPDP 2018, ICT 2018 and CPDP 2019.

- Regarding WP6 Dissemination, being accepted at SAP TechEd 2018 event series was a substantial achievement and a productive industry event dissemination opportunity.

- How privacy-by-design is core to PANORAMIX has been described in D1.5. By engaging with our legal expert, Merel Koning, a formal analysis has been included in D1.5 regarding how current and future users of the Panoramix framework and software could improve their compliance profile with respect to GDPR.

- Regarding standardisation (D2.4), the PANORAMIX project participated in the creation of the Privacy Enhancements and Assessments Research Group (PEARG), a new effort that has led to the recognition by the IETF of the importance of privacy across all new Internet standards and provides a forum for the interaction of industry and academia over issues of privacy in all standards, including but not limited to standardisation of the Sphinx mix-network format, a crucial building block of the Panoramix mix-net. This work by PANORAMIX at the IETF has prepared the way for future standardisation of mix-nets at the IETF after the end of the project.

- The integration of two modern, fast mix-nets in Panoramix to enable large scale elections. One developed by PANORAMIX partner UT and the other is Verificatum which was developed outside PANORAMIX. The integration of Verificatum is a particularly important achievement, as it shows that the framework developed inside the project is interoperable with technology developed externally.

- A spin-out from the project is already in motion as the new entity, Nym Technologies SA, has been created. It is one of the ways the results of the PANORAMIX project will continue to be exploited beyond its the conclusion of the project. At the same time PANORAMIX partners have leveraged on the success of the project to attract additional funding such as the H2020 project PRIVILEDGE as well as industry funding such as the Samsung NEXT Stack Zero Grant.

2.3 Milestones Reached & Completed Deliverables

In the final year of the project, the following milestones were reached (milestones MS1-MS5 were achieved in Y1, and MS6 & MS7 in Y2, see Deliverables D1.2 & D1.2):

- (MS8) Integrated mix-net system
- (MS9) Second Iteration and Security Analysis Report
- (MS10) Final System and User Feedback Analysis

All of the deliverables required according to the DoA were completed on time with only minor deviations.

- D1.3 – Final Review and Assessment (Editor: UEDIN) [M41]
- D1.5 – System Abuse / Misuse and Mitigation Strategies (Editor: UEDIN) [M41]
- D2.4 – Standardisation Report (Editor: GH) [Due: M41]
- D2.7 – Report on Exploitation Activities and Updated Plan for Further Exploitation (Editor: GH) [M41]
- D2.8 – Scientific Advisory Board Reports (Editor: UT) [M41]
- D2.10 – Dissemination Report III (Editor: UEDIN) [M41]
- D3.3 – Final Report (Editor: UCL) [M30]
- D4.3 – Integrated System (Editor: KUL) [M29]
- D4.4 – Final System (Editor:KUL) [M41]
- D5.3 – Integrated System (Editor: GRNET [M29]

- D5.4 – Final System (Editor: GRNET) [M41]
- D6.2 – Final Report Validation & Testing (Editor: SAP) [M41]
- D7.2 – Open-source code of integrated system for desktops (Editor: GH) [M29]
- D7.3 – Analysis of User Feedback (Editor: GH) [M41]

3. Final 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 second periodic review and then goes into more detail how the progress towards objectives was achieved for WP1 in the final year. A number of recommendations were given after the periodic review concerning the period covered by the Y2 report, in short these concerned:

Periodic Report and D1.2 These documents were revised according to the recommendations given and the advice has also been taken on board for the current deliverable.

Evaluation and Measurement. Evaluation metrics for all three use-cases are included in the final deliverables. The current deliverable also addresses the various aspects of the project according to the objectives and target numbers defined on DoA p.24.

The website. In order to better support the exploitation targets of the project we have opted to have and/or contribute to three separate websites with different objectives, namely:

1. `panoramix-project.eu`: EU-commission style project web site
2. `panoramix.me`: a user friendly public-facing web site for PANORAMIX outputs
3. `mixnetworks.org`: a developer facing web site, for developers interested in working with mix-nets.

Review and Resubmission of Deliverables. A number of deliverables were reviewed and resubmitted. The resubmissions were completed by December 15, 2017 and formally approved by February 1, 2018.

There were also a number of recommendations concerning future work, which we have incorporated in the running of the PANORAMIX project during the final year as follows:

Communication, Dissemination and Exploitation Overall, the project has focussed to a great extent on the expected outcomes, and their adequate exploitation. As recommended, the final dissemination and communication plan (D2.10) includes an extra section which provides detailed information about all the groups that are potentially interested in the project's results and specifies the actions taken for disseminating the project's results towards these groups. Furthermore, the exploitation report describes all the steps that have been taken to ensure the exploitation of PANORAMIX beyond January 2019.

Networking D2.10 (Section 3.4) lists all the networking activities that were undertaken with other H2020 projects over the course of the final year. For example, we took part in the European Privacy and Data Protection Summit (CDP) in Madrid which had a special session on H2020 projects organised by the H2020 project TYPES. PANORAMIX was also one of 25 H2020 projects presenting at the H2020 Project Clustering Workshop organised by H2020 project ReCRED.

User Engagement The user engagement studies for WP7 have been ongoing from late spring 2018 until December 2018, to ensure we were able to canvas as diverse a population as possible for the messaging use case.

Security and Privacy Considerations and EU regulations To show how the project complies with EU regulations and how the technical output of the project has been developed with security and privacy principles in mind we enlisted the help of a legal expert, Merel Koning, to analyse PANORAMIX from a GDPR perspective and to draft part of D1.5. In addition to Merel Koning, our ethics advisor Joss Wright provided guidance from an ethics point of view.

Task 1.1 – Project Coordination and Communication: 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 (PSC) are present at these meetings as well as any consortium members that are available to attend.

There have been two face-to-face meetings since September 2017. The External Advisory Board members were invited to both meetings as well as interested key representatives from stakeholder groups. The first meeting was held in Brussels in January 2018 to coincide with the PANORAMIX panel at CPDP. We were joined by Marit Hansen and Gus Hosein from the EAB, as well as Merel Koning (legal advisor), Carmela Trancoso (NEXTLEAP), Zaki Mannian (cryptocurrency investor) & Privacy Camp attendees. The second one was held in Athens in September 2018, with the main goal of ensuring the whole consortium was up to date and on schedule to complete well in time for the final review meeting in January 2019. Two different

members of our EAB were able to join us: Bart Preneel and Sven Heiberg as well as members of the Athens privacy and security community and members of the Nym spin-out.

In May 2018, there was a change of the PANORAMIX Project Officer at the European Commission. Thus the communication has taken place with two different officers. In addition to sharing regular project information with both project officers, permission was sought to engage a legal expert to assist with our legal analysis and compliance profile (D1.5). The outcome was that this was possible without an additional amendment as the PO did not consider this change to constitute a significant change to the Annex 1, enabling us to benefit from the simplified approval procedure. Communication with the new PO has centred around the ICT meeting which took place in December 2018, EIPP marketability questionnaires for the project and a schedule for submitting drafts of all the M41 deliverables well before the official submission date of January 31, 2019.

Task 1.2 – Resource Control: The coordinator has been monitoring the use of resources of each partner and some transfer of budget between beneficiaries will take place to even out the over- and underspends between partners. In the last WPLB & PSC meeting, a motion was put forward to use the underspend at SAP to cover the overspend at CCT. The motion was accepted with unanimous agreement by the consortium.

Merel Koning, our legal expert, was reimbursed for travel to our meetings and for writing the legal perspective in D1.5. Joss Wright has been reimbursed for his time investment in D1.4 and D1.5 as the project's ethics advisor.

Task 1.3 – Quality Assurance: The project manager in her role as Quality Assurance Coordinator (QAC) has continued to encourage the consortium to stick to the Quality Assurance Plan (QAP). When this plan is adhered to the deliverables are ready well ahead of time allowing for a round of review and revision prior to submission.

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.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0.72	12.33	13.05	7.2
UCL	1	0	1	5.4
UT	0	0	0	0
KU Leuven	0	0	0	0
GRNET	0	0	0	0
SAP SE	0	0	0	0
Greenhost	0	0	0	0
CCT (MV in Y1)	0	0	0	0
UoA	0	0	0	14
Total	3.8	12.33	16.13	26.6

Table 3.1: WP1 - Actual PMs per reporting period and as estimated in the Grant Agreement.

3.1.4 WP1: Deviation from Objectives

Deviations of more than 10% between estimated and actual effort:

- Extra resources were needed at UEDIN to ensure the tasks in WP1 could be executed well. In terms of PMs, the increased numbers in RP2 are due to the appointment of a project manager at UEDIN at the end of Y1.
- Conversely, the PMs at UoA were not fulfilled and respective tasks were taken over by more senior personnel at UEDIN.
- The slightly lower PMs for UCL are due to their assistance not being needed with the WP1 efforts, as the quality control was transferred to the project manager at UEDIN.

3.1.5 WP1: Documents and Deliverables Produced

- D1.3 Final Review and Assessment (Editor: UEDIN) [M41] The current document.
- D1.5 System Abuse / Misuse and Mitigation Strategies Editor: UEDIN) [M41] The report details misuse and abuse scenarios and provides techniques to be followed by partners and any other Panoramix operators to minimize any negative effects of such scenarios. It also includes the legal perspective of PANORAMIX in the context of General Data Protection Regulation (GDPR) and more specifically Data Protection by Design and by Default (DPbD).

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 final year dissemination results are reported in Deliverable D2.10, as in previous years, the targets set for dissemination have been met by the consortium. A few highlights from D2.10 are:

- Specific target groups per use-case have been described in D2.10 as well as how we will continue to engage with these groups beyond the lifetime of PANORAMIX.
- In the final year of PANORAMIX, seventeen papers were accepted for publication at a range of scientific venues. The main group of people reached with this type of dissemination is the research and scientific community.
- Networking opportunities – with other Horizon2020 projects and more broadly – were embraced by taking part in for example: the Congreso de Privacidad (CDP) in Madrid, the H2020 Project Clustering Workshop in Athens, the Cyberwatching.eu concertation meeting in Brussels and culminating in ICT 2018 Imagine Digital - Connect Europe in Vienna in December 2018.
- After the success of presenting the Minimum Viable Product at CPDP 2017 which was received extremely well PANORAMIX proposed a panel: “Anonymous Communications Infrastructures for the Protection of Metadata” which was accepted for the conference in 2018 and was a great opportunity to further present PANORAMIX to a diverse audience comprising the scientific community, civil society, general public and policy makers.
- The justification for the 5-month no cost extension was two-fold, the first was of course that work on WP7 had been stalled, the second was to align better with more widely disseminating the end results of the project to the privacy community at the CPDP conference in January 2019. Getting a panel at CPDP accepted is no mean feat and being able to be part of CPDP again in 2019 is testament to the success of PANORAMIX. The panel for this year is all about the exploitation of PANORAMIX and will be about “Anonymity loves company and funding”.

The PANORAMIX webpages at `panoramix-project.eu` have been kept up to date with regular updates to the publications and blogs describing our news, successes and advertising key dissemination activities. The PANORAMIX twitter feed, (@PanoramixH2020) continued to be used as another way of engaging the wider public with PANORAMIX. In the final stages of PANORAMIX a further website has been set up `panoramix.me` which is there to point interested parties in the right direction regarding the various exploitation activities for PANORAMIX and where to find more information. Finally, there is `mixnetworks.org`: a developer facing web site, for developers interested in working with the Panoramix mix-nets.

Task 2.2 – Standardisation: Deliverable D2.4 *Standardisation Report* gives a comprehensive overview of the standardisation efforts that have taken place during the course of PANORAMIX. To summarize, the creation of the Privacy Enhancements and Assessments Research Group (PEARG) and the recognition by the IETF of the importance of privacy across all new Internet standards has prepared the way for future standardisation of the Panoramix mix-net at the IETF after the end of the project.

Task 2.3 – Exploitation: Deliverable D2.7 is the final exploitation report and describes the progress made over the course of the project by all partners and details future work and further exploitation efforts. D2.7 also details the plan for general purpose exploitation of mix networks, including the creation of Nym Technologies SA which will be exploiting the results of the PANORAMIX project going forward. Nym is exploring new and novel methods for building communities around the mix-net software using token-based incentive structures and detailed plans on how to build off of not only European, but global funding resources.

Task 2.4 – Advisory Board: The EAB was engaged with through project meetings, e-mail communication and teleconferences. The general view of the EAB is that the PANORAMIX project has delivered well beyond what was expected and the level of collaboration between partners was commended. D2.8 lists the interactions with the EAB and summarizes their feedback to the consortium.

3.2.3 WP2: Beneficiary Involvement

For the use of resources in WP2 see Table 3.2. Role of the partners:

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

UT contributed to compiling and editing D2.8 (Task 2.4).

GH managed the exploitation report and the standardisation activities (Tasks 2.2 & 2.3).

ALL partners contributed to the tasks as detailed above and specifically by participating in international conferences, promoting standardization efforts and their exploitation activities (Tasks 2.1, 2.2 & 2.3).

3.2.4 WP2: Deviation from Objectives

The main deviation in WP2 concerns D2.8. The input to D2.8 was slightly different to what was envisioned in the DoA. Following their preference, the EAB did not provide reports after each EAB meeting but rather UEDIN and UT took the feedback that was provided by the EAB - at meetings, through e-mail communication and teleconferences and compiled that into D2.8. Details are given of which members of the EAB attended and the feedback and advice that they provided.

Deviations of more than 10% between estimated and actual effort:

- UEDIN & UoA – The planned PMs from UoA were transferred to UEDIN, i.e., the underspending of resources by UoA in this WP was offset by more resources being used by UEDIN to cover all necessary tasks.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0.48	4.61	5.09	2
UCL	1.21	0	1.21	6
UT	1.6	6.5	8.1	6
KU Leuven	1.5	3.37	4.87	5
GRNET	0	4.14	4.14	16
SAP SE	0.78	5.78	6.56	7
Greenhost	2	4	6	6
CCT (MV in Y1)	5.1	2	7.1	7
UoA	0	1.88	1.88	4
Total	12.67	32.28	44.95	26.6

Table 3.2: WP2- Actual PMs per reporting period and as estimated in the Grant Agreement.

- UT – Slightly higher number of PMs due to the more junior make-up of the workforce.
- UCL – The resources used for dissemination (WP2) at UCL have been included in the reporting for WP3 and WP4, hence the lower than estimated number of PMs.
- GRNET – The WP2 tasks that were fulfilled by GRNET were achieved with less PMs than estimated in the Grant Agreement due to more senior staff involved.

3.2.5 WP2: Documents and Deliverables Produced

- D2.4 – Standardisation Report (Editor: Greenhost) [Due: M41] The standardization-related efforts and achievements are collected in this report.
- D2.7 - Report on Exploitation Activities and Updated Plan for Further Exploitation (Editor: Greenhost) [M41] Final update of the exploitation plan and a list of exploitation activities performed during the last year of the project is reported.
- D2.8 - Scientific Advisory Board Reports (Editor: UT) [Due:M41] After each EAB meeting EAB will write a report with observations, recommendations and conclusions on actions for increasing the project impact. A summary of all reports will be compiled at the end of the project.
- D2.10 - Dissemination Report III (Editor: UEDIN) [Due:M41] Dissemination activities performed in final period.

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

This final phase of Work Package 3 concluded the PANORAMIX activities around research and advanced development, towards mix-nets that support both secure elections, through robust mixing, as well as email and messaging use-cases that require low latency and higher performance.

On the topic of robust mix networks our teams studied a number of topics. We researched even more efficient mix networks designs, in terms of the cost of producing and verifying proofs of correct mixing. Those proof systems require, traditionally, a "secure setup" of initial parameters; so we further studied how such parameters can be generated securely, without any single party being able to corrupt them to gain an advantage (such as including or excluding votes). Finally we studied specials cases of proof systems, for correct mixing, that enable a specific (semi-trusted) entity to very that mixing was performed correctly at lower costs.

On the topic of designing mix systems for messaging we also studied a number of important theoretical aspects of those systems. First we formalized the notion of mix-networks using an established "provable security" framework, leading to definitions of security and techniques for proving the correctness of designs that are compatible with established cryptographic standards. We also looked at the fundamental trade-offs of mix systems, when it comes to resisting traffic analysis, and for the first time provide a rigorous proof of the choices designers have to make between optimizing for low-bandwidth, low-latency and quality of anonymity.

Based on the above we proposed a design for mix-nets based on multi-party primitives – even though the design is of theoretical interest we prove its security properties rigorously and can be used as a starting point for more practical designs. We also looked at key attacks against low-latency anonymity systems, such as those used for messaging, and specifically "fingerprinting" attacks. We proposed a performant de-anonymization attack based on modern machine learning (k-fingerprinting), which is currently the best known attack against low-latency systems. And in a follow-up paper we provide a number of potential defences against fingerprinting, and benchmark them against known attacks (including our own).

In terms of supporting other WPs our teams supported WP4 in terms of specifying the Panoramix mix-net based on our earlier Loopix designs (Katzenpost), as well as the robust mix-net developed and implemented as part of the Zeus election framework.

WP3 has been scientifically a great success, and both the project partners and the commission should be ready and proud to advertise the quality of the scientific outputs of this WP. Specifically, the quality of the research can be validated through the extremely selective venues in which the peer-reviewed research from this WP was peer-reviewed and selected for publication. Some key highlights include, the following publications:

- Debajyoti Das, Sebastian Meiser, Esfandiar Mohammadi, Aniket Kate: Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two. IEEE Symposium on Security and Privacy 2018: 108-126.

  The IEEE Symposium on Security and Privacy is the top research venue on Information Security, with acceptance rates well below 15%.

- Pyrros Chaidos, Olga Fourtounelli, Aggelos Kiayias, Thomas Zacharias: A Universally Composable Framework for the Privacy of Email Ecosystems. Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security Symposium, pp. 191-221.

  Asiacrypt is one of the three flagship IACR conferences. It is a very competitive conference in cryptography with acceptance rate around 20%.[1]

- Vera Rimmer, Davy Preuveneers, Marc Juárez, Tom van Goethem, Wouter Joosen: Automated Website Fingerprinting through Deep Learning. NDSS 2018

  NDSS (stands for Network and Distributed Systems Security) is the top scientific venue on those topics.

[1] See e.g., `http://www2.mat.dtu.dk/people/Lars.R.Knudsen/accrates.html`.

The fact that the research outputs of the project were accepted in such venues, supports the high scientific quality of the work. Besides, it also has the obvious dissemination benefit of exposing our work in front of a world-class audience.

Furthermore, teams involved in WP3 in conjunction with activities in other WPs published a specification for low-latency mix networks that was implemented in WP4 and others, that is now public and available for all to use: `https://katzenpost.mixnetworks.org/docs/specs.html`

Finally, in terms of exploitation, the Loopix / Katzenpost designs have been industrially influential, and a new start-up Nym TechnologiesSA is using these designs as a basis for its commercial offerings.(`https://nymtech.net/`)

3.3.3 WP3: Beneficiary Involvement

The work finalizing this WP3 was performed by UCL, UT, KUL, UoA and UEDIN. More specifically:

UT took the lead in the design of robust mix-nets, the proposal better shuffle proofs, secure parameter generation, and efficient designated verifier proofs. UT also helped in the implementation of these ideas as part of transiting them to the WP4 package. (Task 3.2).

UCL , with the support of KUL, took the lead in proving the fundamental anonymity trilemma (bandwidth, latency, anonymity), proposing new fingerprinting attacks, as well as evaluating the security of fingerprinting defences against our own and other known attacks for low-latency anonymity cases. UCL and KUL also took the lead in supporting WP4 mix-net specification. (Tasks 3.2 and 3.3)

UEDIN proposed the "provable security" definition for mix networks, and also the design of the MPC mixing system that is provably secure. (Task 3.1)

UoA Contributed to developing a framework for email and messaging privacy (Task 3.1).

Table 3.3 shows the use of resources for WP3.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0.96	20.8	21.76	20
UCL	7.05	37.42	44.47	36
UT	18.5	62	80.5	42
KU Leuven	11.7	52.65	64.35	30
GRNET	0	0	0	0
SAP SE	6.1	4.91	11.01	12
Greenhost	0	0	0	0
CCT (MV in Y1)	0	0	0	0
UoA	3.5	9.38	12.88	12
Total	47.81	187.16	234.97	152

Table 3.3: WP3 - Actual PMs per reporting period and as estimated in the Grant Agreement.

3.3.4 WP3: Deviation from Objectives

D3.3 was delayed by a couple of weeks due to a UK wide Universities strike as well as emergency weather conditions which all took place when the deliverable was due.

Deviations of more than 10% between estimated and actual effort:

- UCL – The work carried out at UCL can be categorised as mainly research. The PMs reported by UCL in the participant portal reflect this categorisation. Over all WPs, UCL spent less resources than planned. The split of PMs per WP is different compared to what was envisioned in the grant agreement. For WP 3 & 4 the PMs are higher and in WP 6 & 7 they are lower than planned. However, the research work that was incorporated into the use cases WP 6 & 7 was carried out by UCL, and claimed under WP 3 & 4 as it was deemed that this was the most appropriate way to categorise.

- UT – A different makeup of the local workforce than initially envisioned has led to higher PMs than originally estimated. 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. Furthermore, although their work was actually used across the WPs, UT claimed most of their PMs on WP 3 and WP 5 rather than distributing them as envisioned in the Grant Agreement.

- KUL – The higher number of actual PMs compared to what was estimated is due to lower seniority levels of staff.

3.3.5 WP3: Documents and Deliverables Produced

- D3.3: Final Report (Editor: UCL) [Due: M30] Final iteration of the NIZK shuffle proof together with security analysis, and an implementation; validation of mix-net design options and refinement of definitions to suit other WPs

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

During this year we have produced several prototypes before reaching the stable version of the PANORAMIX API implemented by the Panoramix library. The first versions addressed the most urgent needs of the use cases, with special attention paid to performance issues. Later, we talked to the partners to make sure all their requirements were met, and finally we restructured the API in order to ease the interoperability of our library and the clients of the use cases. At the end, we were able to release an internet service that can be used to demonstrate the functionality the project as a whole is delivering.

Thanks to the cooperation with WP3 partners, we were able to successfully implement state of the art mix networks based on research published within the project. Of special interest has been the collaboration to improve the scalability of the technology as well as the anonymity provided with respect to the latency of the operations. The software architecture chosen at the beginning of the project has proven to be very useful to implement all the changes required as part of the latest iterations of the project, as their design and implementation can be seamlessly integrated into the corresponding services without much impact on other parts of the library.

We have produced a software library that has already been used to fulfil three different use cases successfully. Talking to the different stakeholders, crafting an API that makes sense for everybody, and implementing the infrastructure through a micro-services architecture that made it easy at the end of the project to accommodate the last and very different requirements from the use cases.

3.4.3 WP4: Beneficiary Involvement

Academia UoA, UCL, UEDIN, UT and KUL followed up with the development, testing and deployment of the system to ensure that the integration of the different pieces and the fine tuning of the default parameters provided strong anonymity guarantees and adaptability to the different usability criteria for each of the use cases (Tasks 4.1, 4.2). UEDIN also contributed to the implementation of the MCMix back end (Task 4.1, 4.2).

GRNET implemented each of the prototypes of the software package (Task 4.3), crafted their design taking into account feedback from the other beneficiaries (Task 4.2), and validated the package with respect to the requirements from each use case (Task 4.3).

UT helped to implement a specific type of mix network which was incorporated in the Panoramix package (Task 4.3).

GH validated the prototypes and made sure the requirements related to WP7 were fulfilled (Task 4.3).

KUL organized meetings, scheduled internal deliverables and coordinated the requests coming from the different use case partners.

CCT validated the prototypes and made sure the requirements related to WP7 were fulfilled (Task 4.3).

Table 3.4 shows the use of resources for WP4.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0.24	30.94	31.18	16
UCL	2.42	35.6	38.02	12
UT	1.6	0	1.6	12.8
KU Leuven	3.1	10.07	13.17	10
GRNET	16.31	26.54	42.85	48
SAP SE	0	0	0	0
Greenhost	4	10	14	14
CCT (MV in Y1)	3.2	5	8.2	8
UoA	0	9.59	9.59	30
Total	30.87	127.74	158.61	150.8

Table 3.4: WP4 - Actual PMs per reporting period and as estimated in the Grant Agreement.

3.4.4 WP4: Deviation from Objectives

Deviations of more than 10% between estimated and actual effort:

- UEDIN, UoA – Some of the work from UoA was transferred to UEDIN.
- UCL, UT & KUL – see the explanation given under WP3; the exact the same reasons apply to the deviation exhibited in WP4.
- GRNET – The tasks fulfilled by GRNET were achieved with less PMs, due to higher seniority staff, than estimated in the Grant Agreement.

3.4.5 WP4: Documents and Deliverables Produced

- D4.3 Integrated System (Editor:KUL) [Due:M29] A fully integrated, tested, and documented system, incorporating any updated requirements and designs from the experience of the MVP that can be disseminated.
- D4.4 (Editor:KUL) [Due:M41] A production-ready system and a corresponding internet service incorporating any external feedback and addressing any remaining integration issues.

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

The objectives set out at the beginning of the project were achieved.

1. The most challenging objective, from a technological point of view, was to evolve the e-voting platform so that large scale elections with hundreds of thousands, even millions of voters, can participate. This was achieved, thanks to the integration of new, advanced mix-nets in Panoramix and the Zeus e-voting service. In particular, two modern, fast mix-nets were integrated: one developed by the UT, and one, Verificatum, developed independently of PANORAMIX. The integration of Verificatum is a particularly important achievement, as it shows that the technology developed inside the project is interoperable with technology developed externally; this also demonstrated how it is possible to integrate other mix-nets in a similar way.
2. A front-end service for voters to cast their votes is fully operational. The service uses web-based technologies and we have verified, through real-world elections, that it can be used from users on desktop computers, tables, and smartphones.
3. A tool for verifying votes has been developed and deployed. The voter can start the tool and provide as input the digital receipt sent when a vote is cast. The tool checks the cryptographic groups and will indicate whether the vote has been counted correctly or not. The tool was of particular interest in a high-stakes election in Romania, where Zeus was used to elect the candidates for the European Parliament elections of the Save Romania Union party.

3.5.3 WP5: Beneficiary Involvement

GRNET (lead) coordinated the work carried out in WP5. It carried out the development required for the integration of the Zeus e-voting platform and Panoramix. It worked together with the UT to implement a production-ready new mix-net.

UT carried out the research and contributed to the design of the new mix-net (Task 5.2). Then, it worked closely with GRNET to ensure that the implemented version of the mix-net matches exactly the theoretical description of it and the original reference implementation.

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

Table 3.5 shows the use of resources for WP5.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0	2	2	4
UCL	0	0	0	0
UT	0.5	28.95	29.45	16
KU Leuven	0	0	0	0
GRNET	20.62	31.37	51.99	62
SAP SE	0	0	0	0
Greenhost	0	0	0	0
CCT (MV in Y1)	0	0	0	0
UoA	0	0	0	14
Total	21.12	62.32	83.44	96

Table 3.5: WP5 - Actual PMs per reporting period and as estimated in the Grant Agreement.

3.5.4 WP5: Deviation from Objectives

Deviations of more than 10% between estimated and actual effort:

- UEDIN, UoA & UT – the tasks envisioned in the grant agreement to be carried out by UEDIN and UoA were, for the most part, covered by UT. This was deemed as more appropriate given the composition of the teams in the respective organisation.
- GRNET – The tasks fulfilled by GRNET were achieved with less PMs, due to higher seniority staff, than estimated in the Grant Agreement.

3.5.5 WP5: Documents and Deliverables Produced

- D5.3 Integrated Syste m(GRNET [Due M29] The integrated service implements the full feature set and incorporates adjustments after the experience with the MVP.
- D5.4 Final System (GRNET) [Due M41] The final version of the e-voting service, fully documented for developers and users, and proven in production conditions.

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 final phase of the project, SAP has finalized their system's implementation (Task 6.2) and began integrating the Panoramix mix-net (Task 6.3) into their demonstrator from work package 6 (WP6) with the assistance of the academic partners UEDIN, UT and UCL. After the integration was finished, SAP started their validation and testing (Task 6.4) efforts in order to evaluate the performance, accuracy, usability, confidentiality as well as anonymity of the system including benefits and effects of mix networks and differential privacy as privacy protection technologies.

According to these tasks, we have performed the following activities:

1. We have finalized our demonstrator and fully integrated the latest version of the Panoramix mix-net. This allows us to collect data from several taxi clients over the mix network instead of direct network connections, thus providing protection for communication metadata.
2. We have designed and performed several experiments to measure the benefits of both the mix network and the differential privacy technique for location data to improve privacy for the users of the system.

3. We have designed and performed experiments to evaluate the effects on utility of the proposed methods.
4. We have measured the performance of the fully-integrated simulation to see its impact on latency and throughput.

We summarized the evaluation results in our final report (deliverable 6.2) that documents the work conducted in this final phase of the PANORAMIX project. Furthermore, in our report we include lessons learned and provide guidance to future adopters of the system.

3.6.3 WP6: Beneficiary Involvement

SAP finalized their implementation of the WP6 demonstrator and fully integrated the application with the Panoramix messaging mix network. They devised utility metrics to compare the quality of analysis results based on original and obfuscated data. Furthermore, they implemented and evaluated membership inference and religion inference attacks to analyze the effects of using differential privacy and mix networks on accuracy and performance and to demonstrate the benefits of using these privacy-protective technologies as countermeasure for these attacks. Moreover, they analyzed the performance in terms of throughput and latency of the integrated system. Lastly, they compiled the results into the final report (D6.2) and provide lessons learnt and guidance to future adopters.

UCL discussed possible improvements to the used location privacy mechanism. Furthermore, UCL performed research towards privacy-preserving surveys and statistics.

UEDIN,UT discussed and evaluated design choices on protocol security and deployment.

Table 3.6 shows the use of resources for WP6.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0	3.94	3.94	4
UCL	3.5	0	3.5	18
UT	0.5		0.5	4
KU Leuven	0	0	0	0
GRNET	0	0	0	0
SAP SE	7.93	32.79	40.72	35
Greenhost	0	0	0	0
CCT (MV in Y1)	0	0	0	0
UoA	0	0	0	0
Total	11.93	36.73	48.66	61

Table 3.6: WP6 - Actual PMs per reporting period and as estimated in the Grant Agreement.

3.6.4 WP6: Deviation from Objectives

Deviations of more than 10% between estimated and actual effort:

- UCL & UT – see the explanation given under WP3.
- SAP – The higher number of PMs compared to the estimate in the grant agreement is due to a lower seniority of staffing.

3.6.5 WP6: Documents and Deliverables Produced

- D6.2: Final Report Validation & Testing (Editor:SAP) [Due:M41] This report summarizes the results of the validation and testing including lessons learned. It provides guidance to future adopters of the system.

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 such as the Center for the Cultivation of Technology for the widest possible deployment. Objectives

- *To integrate mix networks into the LEAP open-source client for the routing of messaging protocols such as e-mail.*
- *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 progress that has been made can be summarized as follows:

- The LEAP infrastructure did not get to a sufficient state of maturity to deploy to Greenhost end-users, which prevented a general roll-out of the mix-net to Greenhost end-users. Instead, work was done on the *mailproxy* client.
- The *Katzenpost* fork of K9-mail supports the Panoramix mix-net.
- The parameters were developed by UCL via a mix-net simulator.
- The generic infrastructure was integrated, as above, into even more popular open-source projects like Thunderbird via *mailproxy*.
- The number of users has not reached tens of thousands, but there was extensive user-testing and is available for tens of thousands. Future exploitation should support tens, if not hundreds, of thousands of users.

3.7.3 WP7: Beneficiary Involvement

GH (lead) led this work package, took the lead in writing of D7.3, and dealt with server-side deployment considerations as well as the LEAP/Bitmask desktop client work.

UCL led the work on creating a mix-net simulator that analyses the data-set gathered as part of Task 7.1, contributed their expertise in the Sphinx message packet and the Loopix system in particular.

CCT has been successful in replacing MV, leading the Android work and core contributors the mix-net programming.

KUL has provided extensive advice to CCT on aspects of mix-net design.

UoA published with UEDIN a formal analysis of the security and privacy properties of the mix-net e-mail use-case.

UEDIN led the formal analysis of the security and privacy properties of the mix-net e-mail.

Table 3.7 shows the use of resources for WP7.

Partner	PMs RP1	PMs RP2	Total PMs	
			Actual	GA
UEDIN	0	2.18	2.18	2
UCL	4.71	0.85	5.56	24
UT	0.5	0	0.5	2
KU Leuven	3.4	7.09	10.49	10
GRNET	0	0	0	0
SAP SE	0	0	0	0
Greenhost	26	82.2	108.2	84
CCT (MV in Y1)	1.5	24.46	25.96	32
UoA	0	3.64	3.64	4
Total	36.11	120.42	156.53	158

Table 3.7: WP7 - Actual PMs per reporting period and as estimated in the Grant Agreement.

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. Due to the change of partners to CCT, there was considerable effort to work on the core mix-net statement and integrate it into a mobile app. As detailed in D7.3, the amount of user-testing done was high but we did not achieve the amount of usage expected. Second, because the LEAP infrastructure did not achieve a sufficient state of maturity to deploy to Greenhost end-users, work was done on the mailproxy client.

Deviations of more than 10% between estimated and actual effort:

- UCL & UT – see the explanation given under WP3.
- Greenhost – The tasks fulfilled by Greenhost were achieved with more PMs, due to lower seniority of staff, than estimated in the Grant Agreement.
- CCT – Due to the deviations explained above, different talent than originally anticipated had to be found and hired, which was more expensive but also much more efficient, which explains the difference in actual PMs.

3.7.5 WP7: Documents and Deliverables Produced

- D7.2 - Open-source code of integrated system for desktops (Editor: GH) [Due: M29] This deliverable, available as code on GitHub with a brief developer guide to the code, will allow system administrators to deploy the mix-networking infrastructure for email, with clients for desktop and mobile (Android).
- D7.3 Analysis of User Feedback (Editor: GH) [Due: M41] Based on the user feedback from the deployment of mix networking with email, we will determine whether or not users found the privacy sufficient. This report will also include the feedback from the living lab research, where the mobile message app is tested with 1000 test users.

3.8 GDPR Implementation for PANORAMIX Use-Cases

This section updates the overview of the GDPR compliance procedures that are implemented by the PANORAMIX partners. The industry partners of the consortium that handle personal data are connected with the three use-cases, which are associated with an industry partner, as shown in the table below.

Case Study	Consortium Partner
Private Electronic Voting Protocols	GRNET
Privacy-Aware Cloud Data Handling	SAP
Privacy-Preserving Messaging	CCT, Greenhost

In each case, the partner has a pre-established relation with its customers and is engaged with PANORAMIX with the only objective to improve the privacy protection of the existing services that are provided to its customers. This will not result in any fundamentally new provision for their users, and as such the underlying data protection agreements are not affected by the new service. Thus, in the below sections we report on the existing data management procedures that are used stressing that these procedures were not put in place for the purpose of PANORAMIX.

3.8.1 Private Electronic Voting Protocols (GRNET)

GRNET operates the Zeus electronic voting platform, which has been in use for over four years. Prior to PANORAMIX, the Zeus platform already provided privacy-preserving electronic voting through a specific mix-net implementation. One of the main goals of PANORAMIX for WP5 is to scale and improve the privacy protections of this platform via its integration with the PANORAMIX mix-net infrastructure (cf. Deliverable D5.3 for details).

The Zeus platform administers the generation and distribution of voters' credentials, vote collection, and posting of the tallying authorities' public data and all other information required for monitoring the election. The implementation procedures are presented in the following table:

Procedure	Private Electronic Voting Protocols (GRNET)
Collection	The electoral committee is responsible for entering the voter registration data (that is, the electoral register). This contains name, surname, father/mother's name, e-mail, phone number. It may also contain an eduGain principal ID. The electoral committee asks the users consent to vote electronically, informing them that their registration data will be stored in an electronic electoral register. The web server hosting Zeus (Apache) keeps a log of accesses and IP addresses. The information on which voters have voted is available to the electoral committee through the Zeus interface, and is consistent with the standard practice in paper ballots, where voter names are stricken off the electoral roll. The web server logs can provide only the access patterns and cannot violate anonymity as everything is encrypted with the election keys. The access patterns may reveal the location of the user when voting.
Storage	The voter registration data are stored in unencrypted form only to be used for future elections.
Protection	The data are protected according to the procedures set by GRNET's Networks Operations Centre; this does not offer any extra protection to voting data, but the voting data that is stored consists only of web server logs, as explained above, and anonymised (through mixnets) ballots and proofs. This information is also downloadable by the electoral committee and could be be published without any inherent privacy risk.
Retention	The users of the system (voters and electoral committee) can access their data (ballots, voter voting data) and download them. GRNET does not have a formal retention or erasure policy yet as such is still subject to regulation for e-voting in Greece; in fact, the to date experience shows that electoral committees request that GRNET will retain voting data, even though no such commitment has been made. As voting data accumulates with the increasing number of elections, a formal GRNET retention policy will be adopted and will be in compliance with e-voting regulation (when legislated).
Destruction	The data are protected by unlawful destruction in the same way that all data in GRNET services are. As explained above, voting data are not treated separately.
Confirmation	The user is informed of every election procedure that his/her data are processed. This is supported via the user's personal mail and verification of the public election transcript.

By design, Zeus is an e-voting system that preserves ballot privacy and integrity verification (end-to-end verifiability) at a high level. On top of this, the updated version of Zeus, as integrated with the PANORAMIX infrastructure, supports a user-friendly yet secure mix-net configuration for non-experts to safeguard elections (cf. Deliverable D5.4 for details), and hence guarantees the protection of participants' sensitive election data.

3.8.2 Privacy-Aware Cloud Data Handling (SAP)

SAP has many cloud-based offerings as part of their cloud platform, including for instance "Vehicle Insights" which allows the creation of new business models with connected car analytics and vehicle telematics. This business solution is closely related to the work performed in WP6 where we used public datasets to evaluate the capability of PANORAMIX to protect privacy.

We stress that the PANORAMIX use-case of WP6 (Survey/Statistics) has no concrete instantiation at the moment. The objective of WP6 is to demonstrate the use and benefits of privacy-enhancing techniques, particularly mix networks and differential privacy, via the simulation of a representative big data scenario that focuses on trip and location data input by simulated taxi clients. For concrete business scenarios, data is collected, processed and stored according to SAP's existing Global Data Protection and Privacy Policy, that for completeness is provided in Appendix A.2 of Deliverable D1.4. The procedures' implementation under the agreement's conditions are summarised in the following table.

Procedure	Privacy-Aware Cloud Data Handling (SAP)
Collection	Data are collected only after the customer's consent and only for fulfilling the specified processing purposes.
Storage	Personal data are stored only for as long as is absolutely necessary for the purposes specified or other legal requirements. Thereafter, personal data are deleted or anonymised. Inaccurate data are corrected or deleted as soon as possible.
Protection	There is continuous monitoring that data processing is in line with applicable law. Every employee and every third party acting on behalf of SAP are instructed that they are not permitted to process personal data without authorisation. If personal data is to be exchanged within the SAP Group or with other companies, it must first be checked whether contractual agreements on data protection and privacy and data security are required.
Retention	Continuous legal monitoring is applied to ensure compliance with any data retention requirements that arise in a case-by-case basis.
Destruction	Continuous legal monitoring is applied to ensure compliance with any data destruction requirements that arise in a case-by-case basis.
Confirmation	Following the terms of agreement, a person affected may, at any time, request information about the data stored on them, its origin, purpose for storing, and recipients to whom the data is passed on.

3.8.3 Privacy-Preserving Messaging (Greenhost, CCT)

As detailed in Deliverable D7.3, the original plan of incorporating PANORAMIX infrastructure into the LEAP platform as a service to Greenhost users was abandoned, due to the gradual withdrawal of LEAP project partners (something that happened outside of the PANORAMIX context). As an alternative solution, Greenhost and CCT collaborated to facilitate the support of PANORAMIX mix-net via mailproxy, namely the Katzenpost fork of K9-mail, that allows users of any e-mail client to use the mix-net. Both partners host a mix-server that is part of the Katzenpost mailproxy, a role that, as we explain shortly, is compliant with GDPR in terms users' data protection.

Greenhost

For the purposes of PANORAMIX, data collection has only been performed on anonymised metadata, with no personally identifying information. The data collection was email metadata over a four hour time period that was provided to UCL in order to help parameterise and design the PANORAMIX mix network. See Deliverable D7.1 for instructions on how the data was collected in aggregate and anonymised. More information about Greenhost procedures are shown in the table below.

Procedure	Privacy-Preserving Messaging (Greenhost)
Collection	Data collection is never performed on an individual, but Greenhost does use statistics on data in order to both identify what services are working and how they are performing. This is captured in article 5.4 of Greenhost's customer agreement, which is explicitly agreed with by every customer of Greenhost.
Storage	Data collected for measuring the performance of PANORAMIX is kept for 30 days. The data is then sent to UCL for analysis, but locally the data are then deleted. An archival copy may be captured by regular back-ups of the Greenhost system, but archives are only kept in general for 6 months. Thus, there is no long-term storage of even anonymised data for PANORAMIX analysis by Greenhost.
Protection	Article 10 states that data will not be gathered without consent and Greenhost is governed by Dutch law which includes the Dutch data protection act. In detail, in Article 10.2 "Greenhost will not take cognizance of data stored by the customer...unless with the Customer's consent, access has been necessary for performance of the contract or Greenhost is required to do so under a statutory provision or authorized order by the authorities. In that case Greenhost will endeavour cognizance of the data to minimize, to the extent with its power and, if possible, inform the customer of this application in an up to date manner."
Retention	Greenhost follows the current Data Protection Regulation, and will continue to follow the GDPR. This gives customers the ability to demand deletion or modification of their data. Greenhost will comply with all Dutch data retention laws. However, currently although it has been debated in the Dutch parliament, there is currently not a Dutch Data Retention directive and so data retention is covered, as noted earlier, by Article 5 of the customer agreement and so data is only retained to optimise services. In general, Greenhost does not retain individual traffic or even IP addresses of its customers.
Destruction	The data destruction policy is covered in Article 10 of the agreement. Note that this right continues after the customer has left Greenhost, as Article 10 states that "The obligation of this article will remain after the termination of the Agreement for any reason, and so much for so long as the providing party can reasonably claim to the confidentiality of the information. Although this is not explicit, "Unlawful destruction" would be a violation of the Contract by Greenhost, as the service contract requires the data be available to the customer by the definition of the Service.
Confirmation	Greenhost logs data automatically when needed in terms of performance, but only in aggregate without individual logs (See Deliverable 7.1 for details). Therefore, Greenhost does not ask the individual customer to confirm if the data is original or correct. However, if a sample of data is collected for performance, any deviations would be detected from other samples and could lead to an investigation. Also, in terms of PANORAMIX, the aggregate anonymized data are also being analyzed by UCL, who should detect anomalies and help confirm our analysis of how email traffic can work with a PANORAMIX-enabled mix net.

As already mentioned, Greenhost is responsible for hosting a mix-server of the PANORAMIX e-mail mix-net. According to the design of PANORAMIX email mix-net, every e-mail message is anonymously routed via a path of three hops/mix-servers (cf. Deliverable D7.2 for details), so that information about the users' personal data is protected against any single mix-server. This

means that the Greenhost server is part of an anonymous e-mail ecosystem that processes data (routing) in a privacy-preserving manner. Overall, PANORAMIX e-mail mix-net is a mechanism that, when applied, provides users with incomparably stronger privacy guarantees than the ones they enjoy when engaging in the conventional e-mail services that are available in Greenhost.

CCT

CCT is a host of PANORAMIX email mix-server, hence its GDPR compliance with respect to this role is similar to Greenhost. In general, CCT processes only anonymised data and not any kind of personally identifying information (PII). Details about CCT procedures are provided in the table below.

Procedure	**Privacy-Preserving Messaging (CCT)**
Collection	There is no data collection of personally identifying information (PII) during the course of the project. CCT collects anonymised usage statistics and survey data, which is aggregated. CCT does not collect IP addresses, names or other PII.
Storage	Anonymised data are collected and stored on systems operated and owned by CCT or on behalf on CCT by authorised partners with data processing agreements conforming to General Data Protection Regulation.
Protection	Only researchers participating in the studies and the research respectively have access to the already anonymised data. Only aggregates are made available to the public or the research partners in this consortium.
Retention	No personally identifying data is collected, so no PII is retained.
Destruction	Anonymised data entries are deleted after the course of the project.
Confirmation	Since the records are anonymised, it is not possible or necessary to notify end-users users of the deletion of specific records.

3.9 Overall Conclusions

This document gave an overview of the work that was carried out in the final year of the PANORAMIX project. We can conclude by reiterating that the objectives set out in the grant agreement have been achieved.

- *Objective 1: Building a Mix-Net Infrastructure for Europe*
- *Objective 2: Mix-Nets for Private E-voting*
- *Objective 3: Mix-Nets for Privacy-aware Cloud Data-Handling*
- *Objective 4: Mix-Nets for Privacy-preserving Messaging*

The legacy of PANORAMIX is looking very promising. The e-voting platform Zeus by GRNET has significantly advanced its marketability due to the project outputs and the number of voters and importance of elections carried out by the system is growing. The anonymised data collection application at SAP has received internal recognition and is on the way to be integrated in core components of user facing SAP products. For messaging, partners CCT and Greenhost are committed in maintaining the mix-net infrastructure, while the creation of the new entity, Nym Technologies SA will ensure the results of the PANORAMIX project in general and the messaging use-case specifically are built upon. Our outputs have also found already uses in industry independently of the consortium as exemplified by the adoption shown in the cases of the Lightning network and Google Deepmind.

At the same time, University partners are engaged in other related EU projects who will be users of PANORAMIX technology such as PRIVILEDGE (UEDIN, UT, GRNET), FENTEC (UEDIN, KUL) and MOSAICrOWN (SAP).