Harry Halpin—Ed. (GH)
George Danezis (UCL)
Helger Lipmaa (UT)
Claudia Diaz (KUL)
Panos Louridas (GRNET)
Benjamin Weggenmann (SAP)
Moritz Bartl (CCT)
Thomas Zacharias (UEDIN)
Pyrros Chaidos (UoA)

Report on Exploitation Activities and Updated Plan for Further Exploitation

Deliverable D2.7

January 31, 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	2018-12-03	HH (GH)	Initial draft
0.2	2018-12-19	HH (GH)	Added partners' input
0.3	2019-01-10	HH (GH)	Added further partners' input
0.4	2019-01-14	BW(SAP)	Review & proofreading
0.5	2019-01-15	HH(GH)	Revision based on review
1.0	2019-01-31	MW (UEDIN)	Final revision and submission to EC

Executive Summary

This deliverable presents the final exploitation results for PANORAMIX. It includes results of joint exploitation objectives as well as the partner-specific exploitation results and future plans, with a focus on the final year of the project as the earlier results were given in D2.6. A current assessment of long-term sustainbility is also given as a conclusion.

The deliverable is structured as follows:

- Chapter 1: The first chapter gives a more accurate overview of the exploitation strategy and results so far for PANORAMIX.
- Chapter 2: The second chapter describes the overall exploitation strategy for PANORAMIX, with a focus on the ICO and cryptocurrency use-cases taken up by the new Swiss entity as the main strategy for joint exploitation, including an analysis of the third-year timeline given by D2.6.
- Chapter 3: The third chapter presents the revised partner-specific exploitation results and future plans. It starts with a list of exploitation strategies that can be used by the project partners as a guideline for formulating their exploitation plans as given in D2.6, and shows how these guidelines were met by the PANORAMIX project. The chapter ends with the individual exploitation plans by the project partners. These include the academic partners and industry partners with focus on their specific use-cases.
- Chapter 4: This short chapter presents the conclusions of exploitation in PANORAMIX and current prospects for long-term sustainability after the end of EC funding.

Contents

1. Introduction

This deliverable reports the final exploitation activities of the PANORAMIX project and the plans of each partner for further exploitation into the future. As a whole, this deliverable is the *exploitation report.* As detailed earlier, the exploitation objective of the PANORAMIX project is the development of a multipurpose infrastructure for privacy-preserving communications based on "mix networks" (mix-nets) and its integration into high-value applications that can be exploited by European businesses and beyond, including the key focus areas of e-voting (WP5), statistics (WP6), and privacy-enhanced email (WP7), with each focus area being ran by one of the industrial partners. The plan was first drafted in D2.5 and revised and completed in D2.6. This final report details the progress made in the plan over the lifetime of the project, and clarifies the future work and exploitation.

The general exploitation plan for the token-based general exploitation of an "open" mix network as well as each of the individual partners plans is given in this report. Various new licensing and intellectual property issues have emerged in the course of executing the exploitation plan given in D2.6. The Panoramix mix-net software of WP4 has, as detailed in D2.6, been provided as open-source, without excluding the possibility of dual licensing for commercial use. However, there have been been issues with the code in WP7 being available only under a free software license, and so joint ownership needs to be transferred to a new affiliate entity for the realization of the token-based exploitation plan. This general token-based exploitation plan is detailed first in this report, and then followed by each partner's exploitation plan.

Lastly, we prevent a detailed future plan for the general purpose exploitation of mix networks, including 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. This should allow the final results to continue to be exploited with a budget similar to the successful onion-routing project Tor, which receives its funding primarily from the United States government.

Finally, the future of mix networking and privacy-enhancing technologies, given landmark new regulation such as the General Data Protection Regulation, seems bright. This exploitation report shows how innovative European research, combined with cutting-edge business models and use-cases, can bring Europe to the forefront of privacy-enhancing technologies.

1.1 Relation to other Deliverables and Work Packages

The exploitation report is the third and final in a series of three deliverables that describe the ongoing exploitation activities of the project. It features updated reports with the performed exploitation activities done during the third year of the project. The documents are as follows:

D2.5 Preliminary Exploitation Plan (Editor: SAP, due: M12): In D2.5, the first version of exploitation plan was presented. It was aligned with the consortium partners' business plans and market evaluation.

D2.6 Complete Exploitation Plan (Editor: GRNET, due: M24): In D2.6, we updated D2.5 with exploitation activities already performed including definition of business models for market adoption of results of the project.

D2.7 Report on Exploitation Activities and Updated Plan for Further Exploitation (Editor: GH and CCT, due: M36): In this document, a final update of the exploitation plan will be presented and a list of exploitation activities performed during the last year of the project is reported.

To review from D2.6, there are four major project outcomes with special relevance for exploitation in PANORAMIX: The first is the open-source mix-net codebase and infrastructure which serves as a basis for the three remaining goals. Namely, these are the industry use-cases to implement verifiable electronic elections, privately collect large amounts of user data, and support private messaging. There are four designated work packages assigned to these outcomes:

Development of Infrastructure (WP4): Employ all the technologies (mix-net specifications, zero-knowledge and differential privacy methods) from WP3 to create a European mix network open-source codebase and infrastructure that can be used by the three high-value applications of WP5-7 during the project, and expanded to up to anywhere from between 5 and 10 other business use-cases from outside the consortium, after or during the course of the project. The work package is lead by KUL with support from all academic partners, UoA/UEDIN, UCL, UT, and with close collaboration of the industry partners of the project, GRNET, GH, CCT, SAP, where GRNET will be heading the software development.

E-voting Use-case (WP5): Apply the mix-net infrastructure developed in WP4 to private electronic voting protocols, where anonymity is necessary to guarantee ballot secrecy, and verifiability is needed for holding fair, transparent, and trustworthy elections. The objective is to provide an e-voting service supporting robust and verifiable private elections that scale up to 100K-1M ballots. This is in line with the experience of one of the industry partners of the consortium (GRNET) who will employ our framework for supporting elections for academic institutions at the national level of an EU member state.

Statistics Use-case (WP6): Apply the Panoramix mix-net from WP4 to support privacy-aware cloud data-handling in the context of privacy-friendly surveying, statistics and big data gathering applications, where protecting the identity of the surveyed users is necessary to elicit truthful answers and incentivize participation. The objective is to support private gathering and real-time evaluation of sensitive data such as traffic or smart city data with about 1M-5M updates daily. This is in-line with the business needs and opportunities identified by one of the consortium partners (SAP).

Messaging Use-case (WP7): 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, allowing two or more users to communicate privately without third parties being able to track what is said or to find out who is talking to whom. Our objective is to support private messaging that scales to 90K-200K users, in-line with the needs to serve the existing user base of existing email/VPN providers and project partners Greenhost (GH) and the Center for the Cultivation of Technology (CCT).

2. Third-Year Joint Exploitation for Long-Term Sustainability

2.1 Joint Exploitation Effort

The exploitation of the project's results continued to be a key element for the success of the PANORAMIX project. To re-iterate from D2.6:

The project team aims to achieve this by

(i) making the mix-net framework publicly available,

(ii) thoroughly documenting and demonstrating the use of the mix-net infrastructure in a number of use-cases that cover comprehensively the spectrum of possible applications,

(iii) involving developers and industry interested parties in our open project meetings, and

(iv) building an open source development community around the mix-net Panoramix framework.

(v) creating a possible way to make the open-source infrastructure financially sustainable via financing using an ICO and a token-based economy for supporting the mix network.

(vi) likely aiding the creation a new organization to last outside the lifetime of the project in order to support the aforementioned token-based privacy economy.

Were these results achieved? The overarching exploitation objective of PANORAMIX of a public availability of the mix-net framework was accomplished via the launching of the mix-net (see D7.3) on servers hosted on the Greenhost infrastructure in the third year of the project, available to the general public to use, along with the open-source tools for setting up mix-nodes and mix-nets finalized by WP4. The team also demonstrated the mix-net, involved developers and built an open source community (see exploitation results of CCT), and created a new entity for long-term financial sustainability of the network via a new high-value use-case, cryptocurrency, whose life will last outside the project and who can bring in independent funding via token sales and other sources. As detailed by each individual partner, the three commercial use-cases all have their own exploitation results and plan that will continue outside the life-time of the project as well given in chapter 3. This showed how, as put in D2.6, PANORAMIX enhanced the creation and support of new products and services in the privacy domain. These products and services will have the potential to offer competitive advantage for entities and organizations that are interested in offering a higher level of privacy to their user base.

The general project exploitation results included, as per the strategy laid out in D2.6:

- **Intellectual property protection**. While the project's main deliverable will be open source and publicly available, it will be made via a licensing type that is consistent with integration in commercial use. The strategy taken was a mix of open-source and GPL licensed code for the messaging use-case, the dual-licensing of GPL licensed code by Nym

Technologies SA is considered an advantage in commercial integrations for the messaging use-case as per the business model of Signal. The classical BSD and MIT licenses were used for all components needed for the integrations of the rest of the use-cases by SAP, GRNET, and future commercial exploitation. The transfer of foreground IP from partners, in particular from CCT, to Nym Technologies needs to be done by the end of the project to assure success.

- The project team performed **demonstrations** at CPDP 2018, ICT 2018, and CCC 2018 in the third year of the project.
- The project team engaged in **transfer activities**, with the help of the legal department of KU Leuven, that allowed the core IP to be shared with the new entity Nym Technologies SA.
- The project team continued to engage in **continuous analysis** of technology transfer opportunities, adjusting to a cryptocurrency use-case but changing the funding model given the downturn in the token market towards the end of 2018.
- The project team **investigated economic benefits** from the impact of the research results of the project via continuous evaluation of the advancement of the research results against the user requirements/needs as shown via the user-testing given in D7.3.

2.1.1 Was Innovation Delivered to the Market?

The plan of the project for delivering our innovations to the market as outlined in D2.6 followed a two-prong approach, i.e. the availability of the framework and its demonstration through specific, relevant and commercially viable use-cases. The mix-net framework as it is deployed in a number of commercial products such as Zeus from GRNET and in SAP, as well as the provisioning of a public mix-net for messaging by GH and CCT. As per the industrial exploitation plans given in chapter 3, these use-cases matured considerably, with GRNET featuring clear success and SAP integration of the mix-net into their larger business strategy, with GH and CCT pivoting towards the Nym Technologies cryptocurrency use-case to support their messaging use-case financially.

2.1.2 Joint Exploitation Plan Update

The Lean Business Model Canvas given in D2.6 is updated for the third year, and partners will continue to investigate its usage for the future after the end of the PANORAMIX funding, in order to monitor the success of their use-cases and Nym Technologies for the joint mix-net.

Problem: Users want improved privacy and anonymity for applications ranging from voting to messaging.

Customer Segment: The customer segment varied per application, helped by the technical guarantee on privacy and compliance with legal regimes that demand privacy such as the GDPR.

Unique Value Proposition: Only PANORAMIX can offer resistance to a global passive adversary and even powerful active adversaries in a real-world networking environment, while also ensuring that all data remains in particular jurisdictions that are compliant with regulations like the GDPR. This makes Panoramix technically better than onion-routing solutions like Tor.

Solution: The Panoramix mix-net finished a generic API that can be "plugged" into a wide-variety of applications.

Channels To promote the joint Panoramix mix-net infrastructure, the third year saw gains. See D2.10 for further details, highlights being:

- In the third year outreach continued at customer-facing events such as Computers, Privacy, and Data Protection (CPDP), ICT 2018: Imagine Digital - Connect Europe and Chaos Computer Congress (CCC).

- Mainstream media events at CSOnline and Coindesk reached tens of thousands of readers.

Revenue Streams Each partner has continued to develop their own revenue stream, as detailed in their partner exploitation plans.

Sustainable Competitive Advantage: Although new mix-net research is rapidly emerging in the United States, Katzenpost is the first real-world mix-node.

Key metrics: The key metrics defined can now be given concrete numbers:

- Amount of network (bandwidth) traffic: *Dependent on use-case*
- Number of nodes in the mix node. *Six nodes in public mix-net, described per D7.3.*
- Number of applications known to use Panoramix. *Zeus, SAP analytics, Katzenpost, mailproxy*
- Number of anonymized access tokens in circulation and value of that token *token has not yet launched*

Cost Structure: The main cost is running the mix-net nodes, which will require bandwidth that approximately scales to its usage, as well as developers. Nym Technologies SA has agreed to hire developers like David Stainton with their funding, and the cost of the mix-nodes is still on the order of hundreds of euros a month, and so within budget for CCT and GH, as well as Nym Technologies SA.

2.1.3 Project Community

The events, including open project meetings and open-source meetings, were continued in the third year of the project. Although the project meetings are finished, open-source meetings will continue with hosting possibly by CCT (given external funding) and by Nym Technologies SA. The key organizational, outreach, and developer sprint events outlined in D2.6 in the third year were completed:

- *January 2018* **Organizational Meeting**: A new organization, Nym Technologies SA, was founded, sharing members of the Advisory Board with PANORAMIX members, with the details discussed at the PANORAMIX Consortium meeting in Brussels on January 23rd.
- *January 2018* **Outreach: Computers, Privacy, and Data Protection (CPDP) 2018** At the largest group of potential organizational partners in Europe interested in privacy, PANORAMIX hosted a panel on anonymous communications.
- *March 2018* **IETF**: Panoramix was presented to the IETF for standardization the SAAG, eventually leading to the Privacy Enhancements and Assessments Research Group. See D2.4 for details.
- *September 2018*: **Open Organizational Meeting**: The PANORAMIX project hosted its open developer meeting, attracting students from a nearby E-CRYPT CSA summer school and was a joint meeting with Nym Technologies SA.
- *September 2018* **Developer Sprint: Greece** This developer sprint, organized by CCT, developers from GRNET, GH, and CCT are meeting in Athens to finish the integration needed for WP7 and WP4.
- *December 2018* **Outreach: Chaos Computer Congress (CCC) 2018** User studies of the messaging framework (see D7.3) aand token-based system and a presentation and panel at Nym Technologies SA.

- *January 2019* **Organizational Meeting**: Nym Technologies will meet for planning finances after the end of European Commission funding in January 2019 before the final review.

- *January 2019* **Outreach: Computers, Privacy, and Data Protection (CPDP) 2019** The final results of PANORAMIX and future roadmap for autonomous work by Nym Technologies will be presented in the panel "Anonymity loves company - and funding."

Given the success of the creation of Nym Technologies SA as a an autonomous entity capable of organizing a developer community and deploying its software with both commercial and non-profit partners, and with the success of each partner's exploitation, Panoramix will continue to be a success after the end of the funding, even after the end of open organizational meetings via a developer community and the standardization effort at the IETF, including the new Privacy Enhancements and Assessments Research Group.

2.1.4 Progress on Token-based Business Model for Long-Term Sustainability

As planned in D2.6, a new entity, Nym Technologies SA, was created in Switzerland to exploit the results of the PANORAMIX project. The primary strategy was to develop the tokens providing a way to incentivize the mix-net servers and software development outside of the lifetime of the project. George Danezis and Aggelos Kiayias serve on the board, and Claudia Diaz is in process of joining. Nym Technologies SA is creating a clean separation between the token and blockchain ecosystem from the core mix-networking libraries by virtue of having the further development of the mix-net happen in separate organizations as needed, with Nym Technologies SA focusing on the token use-case.

Nym Technologies SA has already attracted investment, including the backing of the Binance Labs Incubator and investment from German blockchain investors *1kx*.[1] Nym Technologies currently maintains the services of the Swiss-French law-firm LEAX that specializes in cryptocurrencies.[2] Furthermore, Nym Technologies has begun working with Swiss KYC specialists and crypto-exchange Bity in order to guarantee full compliances with fiscal regulations around tokens both in Switzerland and in Europe.[3] Nym Technologies is domiciled in Neuchatel, Switzerland and maintains an office at their new blockchain innovation centre, having established a good relation with the local economic promotion minister. Nym Technologies, having obtained currently over 300K euros in follow-up funding, has now attracted well-known Bitcoin developers and former students of PANORAMIX professors (such as Jedrzej Stuczynski, a student of George Danezis). These coders went to the open Panoramix meeting in Athens (2018) and have had meetings with Aggelos Kiayias in order to help them solve the problems facing them as coders.

Due to market conditions being unstable around tokens, the current plan for the token sale has been delayed, although the process of communicating with FINMA has begun led by LEAX. In general, the date of the token and precise token economics cannot be predicted due to a general market downturn over 2018. However, there is still keen interest from token funds and users in Nym Technologies SA, and so we are confident that this is one of the few token sales that may succeed in 2019. In order to comply with a changing regulatory landscape, the token and credential needs to be functional, or at least 80% functional, before launch. While the precise token economics and their relationship to mix-nets is still a topic for research after the end of the PANORAMIX project, the concrete code to make the token has already been started and should be operational by mid-2019. Due to the issues around tokens, the ability to take "anonymization fees" from cryptocurrency transactions that are sent over a mix-network via specialized cryptography wallets is also being explored by Nym Technologies SA. These fees can

[1] http://1kx.network

[2] http://leax.ch/en/

[3] https://bity.com

then be used to incentive the mix-nodes, likely via their transformation into tokens. The next step will the development of a “proof of membership” certification procedure for moving the initial federation to an open decentralized federation eco-system.

3. Individual Exploitation Plans

3.1 Overview

This chapter contains the individual exploitation reports by the project's partners. These reports note the work done in the last year project of the project, and should be in line with the final plan presented in D2.6.

3.2 Exploitation Results as per Guidelines

As per D2.6, the exploitation plan lists a number of guidelines in order to ensure the sustainability of the project's results beyond the project end and to demonstrate how PANORAMIX has influenced the EU landscape. These include:

1. *Financial exploitation*, building products, projects, or services based on the project results;
2. *Research & development*, by engaging new projects (EU-funded or sponsored by other sources), based on the experiences gained in the project;
3. *Education*, e.g. courses, at the university level or in continuing education, etc.;
4. *Community-building* around the topics of the project, raising awareness for the addressed problems and the proposed solutions;
5. *Knowledge transfer*, from academia to industry, by collaboration or via employees;
6. *Contributions to open-source projects* and *standardization*, providing public access to the mix-net framework and encouraging its broad adoption in commercial and public systems for interested parties.

For each of the general points given in the guidelines of D2.6, we list how the partners in the results have accomplished the goals.

3.2.1 Guideline for Industrial Partners

General strategy

- *Focus on the main results from the project (products, services, ...) and their commercial viability.* Each industrial partner has done a thorough market analysis, as given in D2.6, and executed, as given in their individual results.
- *Consider new business and operating models that become possible with the project for bringing the project results to customers. Explore the role of 3rd parties (not participating in the project) in this scenario.* The new token-based business model has been explored and a new third-party entity, Nym Technologies SA, has been created to exploit the results.

- *Identify drivers for a successful exploitation and consider how those drivers can be harnessed and strengthened.* The drivers of increased privacy due to GDPR have been analyzed and explored.

- *If there are obstacles to a successful exploitation of the project from today's perspective, address them early on.* A number of licensing issues in WP7 have been identified and addressed.

- *Put a strong focus on how European stakeholders (customers of cloud services, providers of cloud services) can profit from the exploitation of the results.* This is reported in detail in the exploitation plan of SAP.

- *Develop a timeline for exploitation, showing how the exploitation can be structured in phases. Identify the prospective time frame after the end of the project to bring the results to the market.* This was done by each industrial partner and the token-based exploitation plan that continues after the lifetime of the project.

- *Identify concrete customer needs that are addressed with the solution and product, and describe ways to quantitatively measure the success.* This is underway by each industrial partner.

- *Involve marketing, product-management, and sales departments early on in the process.* As detailed in the results of each industrial partner.

- *If possible, start exploitation of intermediate results already during the project.* As detailed in this report, this has already started.

- *Consider synergies for exploitation with other projects, possibly also funded ones.* Work between PANORAMIX and the EC-funded NEXTLEAP has already helped in standardization, as given in D2.4.

Economic factors

- *Aim at a quick access to the market. If necessary, create new markets for a successful exploitation.* The new market identified by tokenization and cryptocurrencies is a prime example of this.

- *Address the market for exploitation today (market analysis, prognoses, technical developments).* This was demonstrated in D2.6.

- *Assess the competition for the developed results, in Europe and worldwide.* This is accomplished via open source and analysis of market-gaps of competing projects, such as Tor, that are dependent on US government funding.

- *Provide innovation in project results, ensure there are advantages compared to competitors.* It is inarguable that mix-nets provide a better security and privacy model than the nearest competitor, which is Tor. There is not enough information yet on the Elixxir project by David Chaum to assess advantages and disadvantages.

Scientific and technical goals

- *Assess the impact of general technological progress on the exploitation scenarios.* Although there has been new research on mix-nets, the PANORAMIX project still appears to be cutting-edge compared to efforts from the United States such as Vuvuzela from MIT, which have not been followed up from a research perspective.

- *Pay attention to non-technical developments (legal aspects, privacy aspects, ...) and their influence on exploitation.* This is detailed via the careful analysis of GDPR reported in the ethics report (D1.5).

Intellectual property

- *Consider to protect intellectual property, for example, through patents.* SAP and GRNET have filed patents, and CCT, GH, and the academic partners have not and so have explicitly allowed their exploitation in the new tokenization business.

3.2.2 Guideline for Academic Partners

Academic impact and education

- *Offer seminars, lectures, lab-courses and the-like with topics related to the project. Let the results of the project influence and/or improve education and training.* This is done by KUL, UCL, UEDIN and UoA.

- *Consider to exploit the research in the project for improving the contributions to European research, like building scientific communities, organizing or participating in workshops and conferences.* This is detailed in the Dissemination Report D2.10.

- *The project should help to attract new researchers and students.* New students have been attracted at both KUL and UCL due to PANORAMIX funding.

- *Engage in improved dissemination activities through the project, for presenting work in conferences (industrial and academic), journals, and so on.* See Dissemination Report 2.10.

- *Explore new scientific communities or try to get into other, relevant communities.* This is exemplified by the academic interaction at the CPDP conference, whose latest PANORAMIX panel in 2019 is focussed on exploitation of the results.

Sustainability

- *Make the results of the work available as open-source.* All results are in an open source license of WP4 and WP7.

- *Contribute results to established open-source projects.* See D2.4 for standardization.

- *Invest in maintaining the project results after the project ended.* UEDIN will maintain the website and the investment in the new affiliate entity, Nym Technologies SA, will also continue after project's end.

- *Plan follow-up projects the build on the results.* This is shown via funding from *1kx* for Nym Technologies SA.

- *Form new relations during the duration of the project and engage with new partners in future collaborations.* Interest from new foundations such as the Web 3.0 Foundation shows the potential of new partnerships.

- *Exploit the project for acquiring new projects and further funding.* Many partners, such as KUL and UEDIN, have already begun new funded research grants.

Technology transfer

- *Trigger interest in the industry for your project results.* This is shown by
- *Ensure that students gain valuable knowledge by their work in the project, which they will take to industry.* This is shown in the reports of KUL, UCL, and UEDIN/UoA.

3.3 Exploitation Plans from Academic Partners

In this section, the project's academic partners present their individual exploitation results. This includes courses, new research grants, and the utilization of the open-source PANORAMIX mix-net framework in their research, as well as their contributions to community-driven initiatives of the industrial partners, as well participation in standardization that will continue to attract new parties and potential partners that want to employ or support Panoramix technology.

3.3.1 Exploitation Results of Partners UEDIN and UoA

As public institutions of higher education both UEDIN and UoA are non-profit organizations that will not perform commercial exploitation of the project's results. Nevertheless, both partners have significant benefits to reap from the project results that we outline below.

We present a joint exploitation plan for partners UEDIN and UoA given that Prof. Kiayias who directs the consortium and manages the UEDIN teams also provides guidance to the team at UoA. This reflects the fact that UEDIN was added to the project after Prof. Kiayias relocated from UoA to UEDIN immediately prior to the beginning of the project.

The project team incorporated material and research results of the project in courses related to the topic of the project. Among these are, for instance, the *Computer Security* (INFR10067) and *Introduction to Modern Cryptography* (INFR11131) courses at the University of Edinburgh, as well as the *Computer Security* (YS13) at the University of Athens. This will enhance the course curriculum in the involved institutions with new research and will improve the training provided bringing it up to par with the current state of the art.

The publications on the "MCMix" system as well as on the "Bitcoin Backbone" and "Ouroboros" systems are all considered four-star outputs under "REF-2014" in the UK and thus will be important in the assessment of the University of Edinburgh in terms of national research funding allocation. Furthermore, in 2017, the University of Edinburgh was for the first time selected as an Academic Centre of Excellence (ACE) in Cyber Security Research, an important distinction in the UK for an academic institution that performs research in the area of Cyber Security. The PANORAMIX project was one of the projects that were included in the University's ACE application in 2016 and was a contributing factor to its acceptance.

The PANORAMIX mix-net will be combined with software for e-voting which was developed by a team at the University of Athens using national funding. The system is called Demos (see http://www.demos-voting.org/), and the combination with PANORAMIX will greatly enhance the system's privacy.

Another goal is the deployment of the PANORAMIX messaging system developed in WP7 as an offering in the form of an app that university students can utilize for interacting privately. This will increase the user-base of the PANORAMIX software and at the same time improve the offerings that the University provides to the student population. The deployment is expected to be achieved by the end of the project. It will be a collaboration between two partners, University of Athens, University of Edinburgh and an external partner to the consortium, Technical University of Darmstadt who has researchers collaborating with the the consortium on the topic of private messaging.

Beyond the coordinator, PANORAMIX employs three researchers at UEDIN, Dr. Thomas Zacharias, Dr. Chris Campbell and Dr. Mirjam Wester, and two researchers at UoA, Pyrros

Chaidos and Dr. Olga Fourtounelli. The project provides valuable professional training for these researchers and will enable them to substantially broaden their command of privacy preserving technologies.

3.3.2 Exploitation Results of Partner UCL

UCL is a non-profit educational and research institution. UCL was a leading partner in the research and specification of the anonymous communication infrastructure for messaging in Panoramix. As a result of the Panoramix project we have implemented a number of code bases which we plan to maintain in the future. The Loopix prototype code base, in Python, is already open sourced on Github. We are actively using and extending the code to support experimentation in follow-up projects on anonymity. The petlib and bplib codebases implement basic cryptographic protocols. They have allowed us to rapidly prototype new cryptographic mechanisms and protocols, and now has active contributors from GRNET, EPFL and UCL. We consider those codebases, that resulted from Panoramix, long term assets for UCL and are open to the whole community.

Besides exploiting code bases, we have incorporated knowledge gained as part of the Panoramix project in our Privacy Enhancing Technologies module (which already has exercises based on the petlib libraries). We are also actively pursuing commercialization activities relating to mix networks with Nym Technologies SA, and also follow-up research on payments in mix networks to support modern business models for mix network operators. Those commercial opportunities and potential grant applications are a direct result of the knowledge gained as part of Panoramix.

3.3.3 Exploitation Plan of Partner UT

University of Tartu is a non-profit educational and research institution. UT calls the exploitation successful if the cryptographic tools that the group provides meet a software implementation and if it manages to create an academic community oriented on mix-net research. UT has noted that that the project will have positive impact on the academic community by contributing to PhD theses of the local PANORAMIX members.

Although UT does not plan to run a course fully oriented on mix-nets, it has and will continue run weekly cryptographic seminars which will include topics related to them. Furthermore, it will continue its cooperation with local e-voting companies and provide consulting services when necessary.

UT has exploited the project by creating a solid bound between itself and other partners involved. UT is convinced that tight cooperation between various research organisations significantly increases its chances in participating and running other highly-prioritised security-related EU projects and positively affects quality of research conducted in Estonia.

3.3.4 Exploitation Results of Partner KUL

The design of the Katzenpost system developed as part of WP7 has been included as a one hour lecture in the course "Privacy Technologies." This is a 3 ECTS credit optional course offered by the KU Leuven to students following master programmes in computer science and engineering. In the academic year 2018-19 the course was taken by 18 students. The full description of the course is available in online.[1] The new lecture covers all the design aspects of the Katzenpost system as the state of the art of message-based decryption mixnets.

Concerning follow-up funding applications, the know-how developed within the Panoramix project has been instrumental for participating in a funding application to the DARPA programme "RACE: Resilient Anonymous Communications for Everyone" [2] that aims to develop new types

[1] https://onderwijsaanbod.kuleuven.be//syllabi/e/H09L2AE.htm

of mixnets using multi-party computation techniques.[2] The proposal passed the first stage of review and we were encouraged to submit a full application, which is currently under review.

3.4 Exploitation Plans from Industrial Partners

The industrial partners' exploitation results focus on the three use-cases e-voting, survey data collection and messaging. As these use-cases are clear applications of the Panoramix mix-net, they provide, as detailed in D2.6, even further incentive to maintain the underlying software and infrastructure after the lifetime of the project, as each use-case has clear commercial value. The status of each use-case as a market offering is reviewed in the results given in this section.

3.4.1 Exploitation Results of Partner GRNET

In the third year of the project GRNET has worked on the exploitation of the PANORAMIX results mainly through the Zeus e-voting application, which served ∼65 ballot boxes with a total of ∼34000 registered voters.

The usage of Zeus has increased throughout time, and elections are on a regular basis. Most of the elections are for professional associations, scientific societies, and trade union entities. Among them we can distinguish two uses of particular interest.

1. The Elections of the Medical Association of Thessaloniki took place on October 21–22, 2018. This was a high profile election, and the use of electronic means to conduct it was reported in the media (in Greek). The vote was organized in conjunction with the Aristotle University of Thessaloniki; special care was taken to ensure voters were knowledgeable about the system, and Zeus was modified in order to support the actual voting system that was used. Note that the modifications were not related to the cryptographic core, or the mix-net, but on ballot representation. There were 4 ballot boxes with ∼3500 registered voters each.

2. The Elections for appointing the candidates for the European Parliament Elections of the Union Save Romania (USR) party. USR chose Zeus as it was the only open source system that could meet the voting system requirements, namely, a score-voting system. The elections took place successfully in November 22–29. The Zeus interface was ported to Romanian, while the cryptographic core and the mix-net did not need any modification. There were ∼6000 registered voters.

The Zeus team was also approached by MiVoz, an open source non-profit based in Urugay, and we are currently investigating porting the Zeus interface to Spanish.

On a more technical level, the Zeus and PANORAMIX mix-nets were integrated with the Verificatum mix-net platform (https://www.verificatum.org/). This was a major validation step, as Verificatum was implemented outside PANORAMIX, yet we were able to show that it is interoperable with Zeus itself. The integration of Zeus and PANORAMIX with Verificatum can add significant dissemination leverage, showing that our technical work accommodates and is compatible with related developments undertaken by the e-voting community around the world.

Note that, in general, it is a conscious choice of the Zeus team not to advertise or promote Zeus aggressively, but to rely on word-of-mouth and good past record for its usage to grow. To this point we have been proven right, and we expect even more intensive use of Zeus in the coming year, after the end of PANORAMIX.

3.4.2 Exploitation Results of Partner SAP

SAP has grown to become the world's leading provider of business software solutions. With 12 million users, 96,400 installations, and more than 1,500 partners, SAP is the world's largest inter-enterprise software company and the world's third-largest independent software supplier,

[2] https://www.darpa.mil/program/resilient-anonymous-communication-for-everyone

overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP industry solutions support the unique business processes of more than 25 industry segments, including high tech, retail, manufacturing and financial services. Via Horizon 2020 projects SAP bridges the gap between open, collaborative research with external partners and exploitation into new or existing SAP product lines through SAP's development groups.

The 35+ researchers of the Product Security Research unit focus on security and privacy in the software development process and products. Recent results include, among many others, a searchable encrypted cloud database, an attack monitoring framework for ERP systems, and cloud-based secure multi-party computation schemes for optimization problems in distributed supply chains. The Product Security Research team has a long history of leading European collaborative research projects to success (15+ projects in FP7) and is actively contributing to shaping the security research agenda.

Exploitation Strategy. As part of the PANORAMIX project, SAP was primarily working on the definition, implementation and validation of a use case which relates to a company transitioning its data and business operations into the cloud. An important driver for the cloud business is big data, where large amounts of information are aggregated and analyzed in order to extract value and provide new insights from the processed data.

The demand for data, however, is often faced with the data owners' reluctance to give out their data due to privacy reasons. Depending on the legislation, privacy laws might further prevent sensitive data from being shared or analyzed. Our goal is to provide our customers tools to improve their business while protecting their own and their customers' privacy. To this end, we want to apply technical measures such as anonymization in order to convince data owners to share their data and to fulfill the necessary legal requirements.

Anonymization could allow our customers to leverage client data that would previously have been unavailable for further analysis due to privacy concerns. This could give them better insights into their business or other activities. Enhancing big data applications with privacy-preserving mechanisms could thus provide a unique selling point and advantage over competitors.

We have identified several stakeholders at SAP whose use cases match this big data scenario where data from multiple sources is aggregated in a database in order to be analyzed. Among others, these include

- anomaly detection for enterprise systems,
- evaluation of position data from vehicles (e.g. finding frequent routes), and
- evaluation of customer feedback in surveys or on social media.

In these applications, customers are often asked to share 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 long-term 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. A similar reasoning applies to all our identified big data use cases. In summary, they have the following non-functional goals in common:

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

2. *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.

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

To reach these goals, we applied the following approach:

1. We connected the database to the Panoramix mix network developed in WP4 in order to achieve anonymity. We can trust the mix and even cascade several of them in order to distribute the trust.

2. We used 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.

3. We used an in-memory database in order to provide the performance necessary for data processing.

While we leverage existing in-memory databases to achieve the last goal regarding performance, we can directly utilize the outcomes of PANORAMIX to achieve both privacy-relevant goals, anonymity and data confidentiality, through employing the Panoramix mix-net framework (WP4) and the results on differential privacy (WP3).

As part of the PANORAMIX project, SAP implemented the above approach and demonstrated the use and advantages of the Panoramix mix network in a collaborative (SaaS) application (WP6). We collected data (e.g. sensor data from IoT devices) from a set of predefined (simulated) clients and aggregated 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 wanted to perform the typical big data type of aggregate analysis on them with reasonable accuracy. The objective of WP6 was to equip the database with the necessary mechanisms and connect it to the mix network. In the process, we gained hands-on experience on employing mix-nets and differential privacy, which is indeed eneficial for providing further SAP applications with these privacy-enhancing technologies. As such, the results of the WP6 use cases are perfectly aligned with SAP's business strategy. Furthermore, having a demonstrator at hand allows us to raise awareness of PANORAMIX technology among internal and external stakeholders.

SAP's Product Security Research runs a few internal projects that are fed by a (larger) number of EU projects. This enables us to focus on a few core inventions and innovations we deliver to SAP. The internal research project related to PANORAMIX is called AWARE ("Anonymization With guARantEed privacy") and will also be receiving research output from the C3ISP H2020 project from this year onwards. The goal of AWARE is to investigate and improve methods for anonymization with measurable and reliable guarantees. As such, it mainly absorbed the results from WP3, where SAP has been working on the definition, design and validation of differentially private anonymization methods. These methods feature a privacy parameter that can be appropriately set to balance privacy versus utility. The idea is that differential privacy can be used in conjunction with mix-nets such as the Panoramix framework to protect both the anonymity of the data owners and the confidentiality of the data values themselves.

Having a framework for mix-nets and suitable anonymization mechanisms allows easy integration into other products, thus allowing stakeholders to directly benefit from the outcomes of PANORAMIX. The results of SAP's research efforts within PANORAMIX directly fed into an already ongoing effort to deliver an industrial-strength solution to SAP customers as part of SAP's overall cloud strategy. The SAP Product Security Research group has a full SAP development environment available within which own and partner project results can be tested and deployed. Any generated IP will be either used following a passive (publication) or active (patent filing) strategy. SAP uses and will continue to use open source software in its products and import the Panoramix software in its own development line.

Timeline. In the first year, the goal was to create awareness in the development organization. We participated in developer conferences and hold a management workshop in order to make the stakeholders aware of the on-going project. In the second year, we focused on demand generation and dissemination of our roadmap. We involved decision makers and pilot customers in order to create a roadmap for the productization of PANORAMIX results. In the third year, the goal was to initiate the techology transfer. We thus created a detailed transfer plan and handed over the developed code and documentation to product teams.

Activities performed in the first year. In the first year we followed the plan in order to create awareness. Concretely, the following list presents the exploitation activities that we have performed:

- We have contacted and held meetings with several internal stakeholders, which resulted in a list of SAP products and use cases that would benefit from PANORAMIX outcomes. Among the use cases are

  - anomaly detection in enterprise systems,
  - evaluation of telematics data from vehicles, and
  - evaluation of customer feedback/surveys.

  Follow-ups were planned and further collaboration was performed.

- We have formulated an internal research strategy on anonymization where we address the most promising use cases and needs that we identified during the discussions with our stakeholders. Since the use cases match the privacy-preserving big data analysis scenario we have devised for WP6, the outcomes from PANORAMIX will perfectly fit this strategy. Moreover, we have made sure that our internal research strategy which includes the exploitation of PANORAMIX is in line with SAP's business strategy.

- We held a one-week strategy workshop where we discussed our unit's research agenda. Anonymization, which includes our PANORAMIX research goals, was identified as a major topic during the workshop, and as such has been put on our research roadmap. The outcome of the workshop is communicated to top-level management and board members such as Bernd Leukert, head of Products & Innovations, thus creating high visibility for PANORAMIX and its results within SAP.

- Furthermore, we have performed experiments on a first set of differentially private anonymization mechanisms that could be utilized in SAP's use cases.

Activities performed in the second year. In the second year of the project, we held further stakeholder meetings and discussed concretized plans for productizing PANORAMIX results in order to make them available for prospective pilot customers within SAP:

- We held over three meetings with colleagues and product owners from *SAP Innovation Center Network (ICN)* who are mainly working on machine learning use cases. Their most relevant projects that could benefit from anonymization techniques include resume matching and service ticket matching.
- We met with colleagues from *SAP MEE Industries Utilities* who are involved in *Trade EV*, a research project by the German Federal Ministry of Economics and Technology (BMWi). They are working on a charging infrastructure for electric vehicles. We introduced anonymization technologies and discussed their applicability within Trade EV.
- We discussed the ideas of PANORAMIX, foremost the differential privacy technology, with the central *SAP Data Protection and Privacy Office*. The discussion showed that there already is demand for privacy-enhancing technologies as developed in PANORAMIX to offer privacy guarantees in several SAP business scenarios.

Instead of targeting each stakeholder individually with a custom implementation, we conceived that a more generic solution was desirable to reach a greater number of stakeholders and simultaneously allow them to benefit from our technology. Therefore, we started with the development of an *anonymization microservice* that provides implementations of several differential privacy mechanisms.

We hence have two complementing state-of-the-art technologies at hand that we can offer to our prospective customers: While our anonymization service provides data confidentiality through differential privacy mechanisms, the Panoramix mix-net provides anonymity on the network level. Both technologies can be combined flexibly and therefore allow us to provide an ideal level of privacy to our customers (cf. our business model in **??**). Last but not least, we continued our efforts to raise awareness within SAP to present PANORAMIX to other potential stakeholders:

- We introduced PANORAMIX to stakeholders within SAP by presenting and demonstrating our research results on anonymization at SAP d-kom 2017, which took place on January 11 and 12 in Karlsruhe. SAP Security Research had its own booth at a highly coveted spot, and the event attracted over 6,200 employees plus external visitors from selected partners, customers, start-ups, and students.
- At the SAP Security Summit 2017, we gave a talk on privacy-aware enterprise applications and the use cases enabled by anonymization technologies as pursued in PANORAMIX. Furthermore, we were present at a booth on both days where we gave a demonstration of differential privacy with location data and discussed our research on privacy-preserving methods with visitors and stakeholders. The summit took place in St. Leon-Rot on March 14 and 15.

Activities performed in the third year. In the third year of the project, we intensified stakeholder meetings and formulated a plan for productising PANORAMIX results in order to make them available for prospective pilot customers within SAP:

- We held a series of meetings with colleagues from *SAP HANA Core* and *SAP Security Transfer* who are mainly working on data anonymization use cases. Their most relevant projects that could benefit from anonymization techniques include the communication of privacy guarantees to end-users and differentially private surveys.

- We continuously supported colleagues from *SAP MEE Industries Utilities* who are involved in *Trade EV*, a research project by the German Federal Ministry of Economics and Technology (BMWi). The scope of our consultation comprised the application of differential privacy to forecasting algorithms.
- We presented and discussed the results of PANORAMIX, with customers and colleagues at the *SAP TechEd Global* conference series. The acceptance to TechEd enabled us to perform exploitation in three cities covering three continents: Las Vegas, North America, Barcelona, Europe, and Bangalore, India. The invitation to TechEd and meetings there have once more underlined that there already is demand for the privacy-enhancing technologies developed in PANORAMIX.
- We performed a knowledge-exchange session with the machine learning foundation team within *SAP Innovation Center Network* to share and discuss PANORAMIX findings on machine learning model leakage and the threat of membership inference attacks. The resulting awareness is with high likelihood raising demand for privacy enhancing technologies, such as used in PANORAMIX, in the context of machine learning.
- We furthermore engaged in two joint meetings with the Chair of Information Security at University of Stuttgart and the Research Group on privacy-preserving machine learning at Max Planck Institute Tübingen. While these two academic institutions are not involved in PANORAMIX, they frequently advise companies in respect to privacy enhancing technologies. We agreed to continue talks and transfer results to their joint projects where applicable.
- At the SAP Security Summit 2018, we had a booth throughout the event where we presented our results on privacy-aware enterprise applications and the use cases enabled by anonymization technologies as pursued in PANORAMIX. The summit took place in St. Leon-Rot, Germany, on February 13 and 14.

In the second year we concluded that instead of targeting each stakeholder individually with a custom implementation, we conceived that a more generic solution was desirable to reach a greater number of stakeholders and simultaneously allow them to benefit from our technology. To address this SAP started developing an *anonymization microservice* to provide implementations of several differential privacy mechanisms and release them internally. Anonymity on the network level is provided by the PANORAMIX mix-net. Both technologies are combined and therefore allow us to provide an ideal level of privacy to our customers (cf. our business model that was presented in D2.6).

Patents During the course of the project, SAP filed two patent applications related to differential privacy as used in WP6:

- “Differentially Private Outlier Detection” (application no. US 15/387.052, EP 17001769.3)
- “Method and System for Automated Text Anonymization” (application no. US 15/881.958)

Prospective Exploitation Activities In the aftermath of the project, we plan to further extend our anonymization service that was started in PANORAMIX as part of the upcoming H2020 Project MOSAICROWN[3] in order to provide data confidentiality through differential privacy mechanisms, as well as data integrity through the underlying database. Furthermore, the discussions with stakeholders from *SAP HANA Core* and *SAP Security Transfer* have led to the first transfer activities that aim at integrating support for differential privacy mechanisms in

[3] European Union Horizon 2020 research and innovation programme grant agreement No 825333

SAP HANA[4]. We will continue our efforts to transfer further mechanisms and more research results into SAP's products again as part of the MOSAICROWN project.

3.4.3 Exploitation Results of Partner Greenhost

As noted in D2.6, Greenhost is a successful Dutch Internet Service Provider, specializing in providing secure cloud, domain names, web-hosting VPN, and email hosting services to over 20K users as well as dozens of security critical customers. It took part in the exploitation of PANORAMIX results primarily in order to pay developers to integrate the LEAP codebase and VPN platform into its core system and in order to experiment with hosting cutting-edge privacy infrastructure on its system. In the second year, Greenhost co-ordinated closely with the other partners after the departure of Medialaan and helped with finding the replacement in the form of CCT. We have provided feedback to the technical specifications for mix networking and have done user-studies with their at-risk human rights activists, and helped run demonstrations at CPDP. In the third year, this work continued with user-testing in Greece and at the Chaos Computer Congress in 2018, as well as meetings with customers interested in privacy. In general, the results of beta-testing the Panoramix mix-net were not successful in terms of e-mail and messaging and so a public beta was not announced as planned in 2018, but Greenhost pivoted to providing the core secure server services for the wider Panoramix mix-net, which is in conjunction with the unified exploitation results, and should provide a source of income to Greenhost after the end of the project.

Greenhost was too positive over the potential for mix-net powered secure messaging and e-mail. Earlier, two general market trends were observed in D2.6, one for secure e-mail and another for secure messaging. However, while there is still likely a market for these trends, the user-testing results done with Greenhost users, while promising in terms of interest, showed that the fundamental mix-net software was not quite ready for customer-centric launch. As detailed in D7.3, although some initial parameters were derived from an email data-set provided by Greenhost, the user-testing showed that the latency was still exceedingly high and thus noticeable for end-users, and was found to be unacceptable to customers, as customers would have to "pay" for using the mix-net while, on the customer-facing side, they would have to deal with higher latency. As has been shown, the secure messaging market may be growing globally (estimated at 1.7 billion USD in 2012, with a growth rate of 7%, and thus an estimated value of 2 billion euros in 2016.[5]), it is still difficult to get users to pay for secure messaging and e-mail.

The main deployment strategy was to be able to turn in on the mix-net as part of Greenhost's general user-facing customer as a default option, but this was hampered by the failure of the open-source programmers in the LEAP team to reach a production-ready client and the aforementioned latency of the mix-net, so that as a business decision it was decided not to turn on LEAP as a default option, and the network of LEAP-enabled providers never materialized outside of Greenhost partner *Riseup.net*. Thus, given the inability to launch a user-facing LEAP platform, the Panoramix mix-net was enabled via the *mailproxy* work so that it could work with any e-mail client. However, there was also a decision not to turn on the mix-net as a default option, and not to increase any fees to Greenhost customers, until the mix-net software was more production ready and latency could be more controlled, although it can be installed as an offering to "early adopter" privacy-conscious customers without additional charge. To turn on the mix-net prematurely for all customers would risk losing Greenhost customers to other secure e-mail and VPN providers such as Protonmail in Switzerland, and so lower the revenue of Greenhost. However, it is hoped as the project matures, eventually the Panoramix software will be deployed as an end-user customer-facing offering.

[4] see http://www.sap.com/data-anonymization

[5] http://www.eb-qual.ch/en/assets/Document-s-events/Doc-events-news/Magic%20Quadrant%20for%20Secure%20Email%20Gateways.pdf

Despite the lack of success of exploitation of the user-facing e-mail and secure messaging in terms of revenue, Greenhost pivoted to a new and unexpected revenue model: Providing secure server infrastructure for the mix-net. While the mix-net use-case for messaging may be hard to commercially exploit, the business plan of the new entity to provide cryptocurrency transactions empowered by the mix-net, where the rewards are shared with the mix-nodes, is a promising path for an entirely exciting new revenue model of Greenhost. As a provisioner of nodes, This would allow Greenhost to attract cryptocurrency customers, who like digital rights customers, need secure hosting in general as well. This has led to new customers approaching Greenhost. Nym Technologies SA will use Greenhost infrastructure for its operations, and there is now interest from cryptocurrency customers as diverse as Aragon in Germany and RIAT in Austria, all of whom met with Greenhost at the user-facing testing session at the Chaos Computer Congress in December 2018. Although it is hard to determine at this early stage the outcome of this potential new revenue stream due to co-operation with Nym Technologies SA and new cryptocurrency customers, Panoramix has expanded the customer-base and profile of Greenhost considerably, keeping Greenhost at the forefront of GDPR-compliant secure and privacy-enhanced infrastructure.

3.4.4 Exploitation Results of Partner CCT

In the PANORAMIX consortium, the goal of the Center for the Cultivation of Technology (CCT) is to coordinate the transition of the messaging use-case from a research project into a sustainable, widely used and actively maintained open source project. In the first year of their involvement, CCT bootstrapped the open source Panoramix implementation via attendance of Tor developer meetings, going to hacker conferences like Chaos Computer Congress, and attracting attention and hires to work on the software. In the second year, CCT continued to mature the codebase, so that now there is a vibrant and active community, and thus the codebase can continue without direct funding or support of CCT, and so proves, as CCT's first EC project, that CCT can successfully incubate innovative open source projects with EC funding. This has led CCT to receive a follow-up grant with NL.Net from the EC to help fund privacy-enhancing technologies, and CCT will continue with its mission in the future with the possibility of EC resources.

The Panoramix codebase is already sustainable, having independently received (via CCT) a 50,000 euro Samsung NEXT grant for messaging (via OpenCollective, a non-profit for open source financing), without any expectations of future returns. As detailed in the exploitation results of Greenhost, there is not a clear business model for messaging by itself. However, as detailed in the joint exploitation results around Nym Technologies, there is a clear business model for cryptocurrency-based use-cases to support wider, more non-profit use-cases for messaging in line with human rights and at-risk communities in need of truly privacy-enhanced messaging. The codebase is to be shared by the end of the PANORAMIX project with Nym Technologies SA in terms of open-source licensing and IP, and thus allow Nym Technologies to use cryptocurrency funds to support core infrastructure work. In essence, this allows wealthy cryptocurrency funds to subsidize the use of the mix-net by at-risk human rights activists at no cost to the activists themselves.

In conjunction with other projects that CCT met at the Chaos Computer Congress, such as Ecuador-based Centro de Autonomia Digital, the Samsung NEXT grant will fund a messaging application on top of the core mix-net software to be maintained financially via the Nym project in the joint exploitation plan after the end of the PANORAMIX project. Also, CCT may continue to receive funds by providing bandwidth to the mix-net, with the funds being again provided by the launch of the Nym project. This will allow CCT to continue to focus on supporting new open source projects while continuing to derive funding streams from the work done under the PANORAMIX project.

4. Conclusions

The PANORAMIX project has reached considerable success in terms of exploitation, as shown by this deliverable, both in the case of academia and industry. The future of the Panoramix infrastructure for mix-nets for public usage looks bright. The PANORAMIX project has successfully engaged also with standards at the IETF, including the formation of the new Privacy Enhancements and Assessments Research Group to bring together industry and academia over issues of privacy, such as the proposed Sphinx packet format (as reported in D2.4).

Individual exploitation results have been presented for each partner, including academic partners. The academic partners have already started to integrate PANORAMIX research and open source software into courses and seminars. The work of PANORAMIX has already led to new Ph.D. students such as Rafa Galvez (KUL) and Ania Piotrowski (UCL), who are all on track to successfully complete their doctorates. Every academic partner involved has received new grant funding in terms of privacy-enhanced technology as well, including mix-nets. The dissemination and research "jump-started" by the EC funding will continue to be exploited by each academic partner long after the lifetime of the project.

Individual exploitation results for each of the industrial partners also were reported. This report shows how the commercial impact of the mix-nets on large companies like SAP in terms of analytics has already began, and that PANORAMIX mix-nets give a crucial commercial edge to the European voting business via GRNET. Given the extreme interest in securing voting over the last year, the exploitation of the e-voting use-case is promising. In terms of offering mix-net enhanced email and messaging, the integration of a mix-net into the offerings of CCT and GH has provided new services to human rights activists throughout the world and grown a powerful open-source community.

Although we will not be able to tell if tokenization is the way to make privacy-enhancing technologies sustainable, we have shown through the organization plan how the intellectual property created by the PANORAMIX project can be tokenized, and have created a new third-party organization, Nym Technologies SA, in order to pursue that tokenization in conjunction with other EC funded work, such as the EC DECODE project, and operating to separate the tokenization of the mix-net from the underlying code of the mix-net itself. This innovative legal and business strategy has already shown results in terms of attracting European token investors such as 1kx, a German token fund that has funded Nym Technologies AG. This bodes well for the eventual success of the tokenization strategy and maximizes the flexibility of obtaining funding in the volatile cryptocurrency markets, and so maximizing the chances that the mix-net will reach massive market penetration successfully via decentralization.

The exploitation results show the success of the PANORAMIX project and already demonstrate long-term financial sustainability, which should continue after the lifetime of the project funding. Therefore, academic collaboration, industry commercialization, academic and industry alliances, and community development are assured to continue.