Aristeidis Sotiropoulos—Ed. (GRNET)
Pyrros Chaidos (UoA)
Anna Piotrowska (UCL)
Michał Zając (UT)
Rafael Galvez (KUL)
Panos Louridas (GRNET)
Benjamin Weggenmann (SAP)
Harry Halpin (GH)
Moritz Bartl (CCT)
Aggelos Kiayias (UEDIN)

Complete Exploitation Plan

Deliverable D2.6

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

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2017-06-15	AS (GRNET)	Initial draft
0.2	2017-06-26	AS (GRNET)	Contact persons
0.3	2017-06-26	AS (GRNET)	Draft TOC-proposal
0.4	2017-07-19	RG (KUL)	KUL will teach mix-nets with Panoramix
0.5	2017-07-21	MB (CCT)	CCT exploitation + business model
0.6	2017-07-21	PH (UEDIN/UOA)	Updated for UoA/UEDIN
0.7	2017-07-21	AP (UCL)	UCL exploitation plan
0.8	2017-07-22	HH (GH)	GH financial plan details, reference to Torservers and K-9 mail, business model, updated standards
0.9	2017-07-23	MB (CCT)	Changes to CCT business plan and exploitation plan
0.91	2017-07-24	PL (GRNET)	Revised GRNET exploitation plan
0.92	2017-07-25	BW (SAP)	Updated Y2 activities
0.93	2017-07-28	BW, DB (SAP)	SAP business model
0.94	2017-08-16	BW (SAP)	Review and proof-reading.
0.95	2017-08-23	AS (GRNET)	Addressed comments/proposals from BW (SAP), pre-final adjustments
0.96	2017-08-28	MW (UEDIN)	Addressed remaining comments
0.98	2017-08-30	AK (UEDIN)	Expanded Exploitation Plan Section on UEDIN/UoA
1.0	2017-08-31	MW (UEDIN)	Final version and submission to EC
1.6	2017-12-11	HH (GH)	Revision taking into account EC reviewer comments
1.7	2017-12-11	AK (UEDIN)	Review
2.0	2017-12-15	MW (UEDIN)	Final revision and submission to EC

Executive Summary

This deliverable presents the second version of the exploitation plan for PANORAMIX. It includes a revised version of our joint exploitation objectives as well as the partner-specific exploitation plans. Moreover, it describes the exploitation activities undertaken during the second year of the project. Further exploitation activities will also be reported at the end of the third and final year of the project (D2.7).

The deliverable is structured as follows:

- Chapter 1: The first chapter gives a more accurate overview of the exploitation plan for PANORAMIX.
- Chapter 2: The second chapter describes the overall exploitation strategy for PANORAMIX. It starts with the joint exploitation objectives for the project and follows with the exploitation plan for the PANORAMIX open-source mix-net framework (WP4).
- Chapter 3: The third chapter presents the revised partner-specific exploitation 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. The chapter ends with the individual exploitation plans by the project partners. These include the three use-cases e-voting (WP5), statistics (WP6), and messaging (WP7) by the industry partners GRNET, SAP, and GH/CCT, respectively.
- Chapter 4: The fourth chapter presents business models for each of the three use-cases in PANORAMIX.
- Chapter 5: The fifth chapter presents the timeline in the third-year for the strengthening and long-term sustainability of PANORAMIX after the end of EC funding.
- Chapter 6: This short chapter presents the conclusions of exploitation in PANORAMIX.

Contents

1. Introduction

In this deliverable the second version of the exploitation plan will be presented. As detailed in the project proposal, 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.

The main deliverable of the project – the Panoramix mix-net software of WP4 – is to be provided as open-source and hence freely available after the project's end for future use, without excluding the possibility of dual licensing for commercial use. A key measure of success is the creation of an online community around the Panoramix system that will take over the maintenance of the software for years to follow the end of the project.

The PANORAMIX system will then be integrated into three high-value civic and industrial infrastructures to implement verifiable electronic elections (WP5), privately collect large amounts of user data (WP6) and support private messaging (WP7). Each application is spearheaded and coordinated by one of the industrial partners of the project to maximize exploitation potential (GRNET leads WP5, SAP leads WP6 and GH together with the support of CCT leads WP7). The support of these diverse applications, through a common open source code-base as well as a unified infrastructure, is a unique benefit of the project and will pave the way for wider adoption of our system in products that seek to conform to privacy-by-design principles. Additionally, other exploitation activities will include the monitoring of the business landscape for the identification of new opportunities and establishing contacts with special interest groups beyond the project's own community.

1.1 Relation to other Deliverables and Work Packages

The complete exploitation plan is the second in a series of three deliverables that describe the planned and performed exploitation activities of the project. It will be subsequently updated with the performed exploitation activities 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 (this document), we update 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): A final update of the exploitation plan will be presented and a list of exploitation activities performed during the last year of the project will be reported.

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. Consortial Exploitation Plan

2.1 Joint Exploitation Effort

The exploitation of the project's results is the key element for the success of the PANORAMIX project. The overarching exploitation objective of PANORAMIX is the public availability of the mix-net framework and its integration in commercial and public systems that seek to improve their privacy profile.

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.

We will present the overall exploitation strategy in the following sections of this chapter. In particular, the exploitation activities regarding the Panoramix open-source mix-net framework will be presented in section 2.2.

The project's commercial partners have committed a substantial amount of integration effort in the respective work packages aiming to bring the benefits of our privacy enhancing framework to their user base. The first important part for the exploitation of the project's results has already been completed during the preparation of this proposal: We have identified relevant use-cases, which will serve as validation points throughout the project. The partners have developed comprehensive exploitation strategies for their use-cases; they will be illustrated in the partner-specific exploitation plans in chapter 3.

The general project exploitation strategy also encompasses the following activities:

- **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 industry partners of the consortium will take the necessary steps of protecting the IP generated as part of their individual exploitation effort (to be detailed below).

- The project team will perform **demonstrations** for interested industry stakeholders during the open project meetings specifically aiming into helping them exploit the project's results.

- The project team will engage in **transfer activities** of our findings into the development, product, and service organisations of the industry partners of the consortium.
- The project team will engage in **continuous analysis** of technology transfer opportunities, adjusting the project when necessary in order to ensure the best possible outcome.
- The project team will **investigate economic benefits** from the impact of the research results of the project. There will be continuous evaluation of the advancement of the research results against the user requirements/needs throughout the project with the help of the partners and we will apply adjustments of the project when necessary.

PANORAMIX will enhance 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 organisations that are interested in offering a higher level of privacy to their user base.

2.1.1 Delivering Innovation to the Market

The plan of the project for delivering our innovations to the market is as follows:

- We will make the mix-net framework publicly available on the project web-site. Specifically, we will make available the source code, detailed documentation, as well as an exemplary roadmap for using the framework and integrating a mix-net process within any application. Since the Panoramix open-source framework is a key component for the exploitation of the project, we will highlight the corresponding exploitation plan in its designated section 2.2.
- We will illustrate the framework in our three use-cases, e-voting, survey data collection and messaging. On the one hand, this will provide a direct channel of delivering our innovations to the market as the project's commercial partners involved in the respective work-packages (GRNET, SAP, GH, CCT). This will ensure that our results will have an immediate and positive impact affecting the users of our commercial partners as privacy is among the requirements that their user base currently demands. At the same time these exemplary use-cases were carefully chosen to illustrate the use of the framework from three different angles, thus opening the road for adoption by other entities after the end of the project. Specific exploitation strategies regarding the use-cases can be found in the individual exploitation plans of the corresponding partners in section 3.4.

Using the above two-pronged strategy (availability of the framework and its demonstration through specific, relevant and commercially viable use-cases) the project team anticipates that the completion of the project will find our mix-net framework already deployed in a number of commercial products. UCL partners have experience in deploying mix-nets (e.g., the "mixminion" system[1]) using such a model. Moreover, through the dissemination via conferences, workshops, as well as open project meetings described above, the software and its advantages will reach a wide audience that will be capable of integrating it with minimal effort in additional application settings.

2.1.2 Joint Exploitation Plan

This section uses the standard "Lean Canvas" in order to demonstrate the joint business plan for the PANORAMIX project. This canvas is a variation of the traditional "Business Model Canvas" that focusses more on customer problems and how to deliver to particular customer segments. An explanation of the "Business Model Canvas" approach is online.[2]

[1] http://mixminion.net
[2] https://en.wikipedia.org/wiki/Business_Model_Canvas

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

Customer Segment: The customer segment will vary per application. However, in general the customer segment will be privacy-conscious users and organizations. We can imagine any organization that wants to offer a 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 will have a generic API that can be "plugged" into a wide-variety of applications that customers, both individuals and organizations, will need.

Channels To promote the joint Panoramix mix-net infrastructure, we will:

- Use at first the use-cases of our partners in e-voting, privacy-enhanced statistics, and messaging to show the Panoramix mix-net is mature.
- We will continue to do outreach at customer-facing events such as Computers, Privacy, and Data Protection (CPDP) and Chaos Computer Congress (CCC).
- Due to the significance of the concern over privacy, we will do outreach connecting Panoramix to major mainstream media as soon as the open-source software is mature and the software ready for beta-testing.

Revenue Streams Each partner will continue to develop their own revenue stream, as detailed in their partner exploitation plans. However, the core Panoramix infrastructure will work on deploying an anonymized access token that can be bought for some amount of monetary value. See Section 2.3 for details.

Sustainable Competitive Advantage: Given that a real-world mix-net has never been deployed before, PANORAMIX will have a "first mover" advantage. The PANORAMIX project features the best-known researchers in the area of mix networking, making it exceedingly unlikely another project could replicate the infrastructure into the future. Lastly, the placing of mix-net in the European jurisdiction also is a competitive advantage.

Key metrics: The key metrics will be:

- Amount of network (bandwidth) traffic.
- Number of nodes in the mix node.
- Number of applications known to use Panoramix.
- Number of anonymized access tokens in circulation and value of that token (See Section 2.3 for details.

Cost Structure: The main costs will be running the mix-net nodes, which will require bandwidth that approximately scales to its usage. There will also be the costs of maintaining open source developers to fix the existing bugs on the common infrastructure that individual partners may not fix.

2.1.3 Developer Community

Due to building off of the LEAP codebase by Greenhost for enabling mix-nets in terms of messaging, we have targeted our initial outreach to the developer community from this point of view. In particular, two Greenhost employees were sent to the LEAP face-to-face developer gathering in Sao Paolo, Brazil. The face-to-face was hosted by the multi-national Thoughtworks,

who is also interested in the mix networking infrastructure being added to the codebase and so is a potential partner in development. Outreach has also been done to European programmers via presentations at the OpenPGP Summit in Germany and the general programmer community at EuroPython. Thoughtworks sent one programmer to the first PANORAMIX project meeting at Saarbrücken. We've also built bridges to other communities. Roger Dingledine, the Director of the Tor Project, attended a WP7 meeting (Secure Messaging) involving UCL, KU Leuven, Greenhost, and Medialaan (representing MV) in 2016. Discussions over mix networking and onion routing were very useful, as well as lessons from Tor in community building. This was followed by a joint mix networking meeting co-located with the Tor developers conference in Amsterdam in March 2017, with participation by CCT, KUL, UEDIN and GH, and created the mixnetworking mailing list[3] to interest developers. CCT has led other companies like Least Authority to take an interest in PANORAMIX work as well.

Future open source developer outreach will continue into the third year, as detailed in Chapter 5. In particular, we will continue doing outreach to the business and government community, with a focus on compliance with the General Data Protection Regulation (GDPR), at the CPDP conference, and continue to recruit open source developers at the CCC conference. Copying the organization of the Tor Project, we will have biannual organizational meetings and developer sprints. It is expected that these will continue after the ending of the project, possibly under the aegis of the new organization that will host the token-based economy, as detailed in Chapter 5.

2.1.4 Standardization

Regarding standardization, PANORAMIX has begun communication with both the W3C and IETF. In terms of IETF, communication has been directed via the Area Director of the Security Area, Stephen Farrell. Although he judged that the work was premature for standardization at the IETF 96 meeting in Berlin (July 2016) at this point due to lack of implementation, he did note that if two or more independent codebases with real-world users (such as e-voting via GRNET and messaging via Greenhost) were using standard PANORAMIX APIs, then a BarBOF would be suitable to see if there was sufficient interest from the rest of the IETF. Stephen Farrell gave instructions on how to set a BarBOF and official BOF ("Birds of a Feather") meeting to begin standardization. PANORAMIX partner Greenhost attended the annual W3C Technical Plenary and Advisory Committee meeting in Lisbon in September 2016 as well to determine if the stronger patent policies from W3C around APIs would help, although it seems the PANORAMIX work sits more naturally on the network level governed in terms of standards by the IETF.

In response to the above, KUL, UCL, and CCT have begun collaborating on a group of specifications that can serve for independent implementation of the mix-net messaging use-case, based on decryption mix-nets and the Sphinx packet format. Already, there are two independent code-bases implementing Sphinx (in Python from UCL and now one in Rust by CCT). Furthermore, a non-compatible Rust variant is under development by Inria for GNUnet, and there has been engagement and interest from the developer community around the Tor Project. Therefore, a pre-standardization mailing list was set-up to co-ordinate the development between implementers of mix networking for messaging. Via GH, PANORAMIX communicated with the Security Area Director Eric Rescorla (Mozilla). His advise was to finish the pre-standardization specifications and submit them as well as the working code from D7.2 once there were two interoperable clients (such as K-9 Mail by CCT and the LEAP Pixelated client by GH) with real users.

Looking into the third year, a BarBOF will be hosted by the IETF. The current plan is to hold the next BarBOF in London at IETF 101 March 18-23 of 2018. Therefore, if successful, standardization could start before the end of the PANORAMIX project at the IETF after another formal BOF is called at the July IETF meeting. This would lead to working IETF standard after

[3] mixnetworks@lists.mixnetworks.org

the project is finished, but would allow the Working Group to form while the PANORAMIX project is still continuing, which would continue to meet quarterly per year as detailed on the IETF homepage.[4]

2.2 Open-Source Mix-net Framework

There is a strong preference in the cryptographic community, and beyond, for open source software implementing published cryptographic protocols. Such preferences may play a very important role in the adoption of new applications—for instance, people with privacy concerns balk altogether against using any closed, proprietary, e-voting solutions.

PANORAMIX will develop a mix-net framework (WP4) that will be entirely available as open-source software. All code, including cryptographic primitives, any libraries that will need to be developed, and any supporting code, will be released in the project repository.

That means that apart from releasing the code under an open source license the code development and evolution itself will be public from a repository service such as GitHub. This will allow third party developers, researchers, and academics, to inspect our implementation and verify that it is correct and faithful to its specifications. The code will be accompanied by comprehensive documentation.

To spread the use of PANORAMIX we aim at involving the open source community closely with our project. To this end, we plan to involve developers and interested parties from the industry to our open project meetings. Ideally, our initiatives would lead to the formation of an open-source development community around the PANORAMIX mix-net framework. We have already had joint meetings with popular open source projects such as the Tor Project and have attracted considerable interest from other companies such as Least Authority.

Currently, CCT is leading these efforts with UCL, KUL, and GH in building a set of specifications for mix networking. We expect as soon as the specifications and initial code-bases are mature and interoperable with existing Panoramix APIs, momentum in the open source community and open standards bodies will allow the Panoramix codebase to flourish.

2.3 Initial Coin Offering

2.3.1 Background

One concept to have privacy-enhancing technologies become financially sustainable is to engage with the current movement towards funding new technologies via blockchain systems. The concept is itself not new, as onion-routing systems such as Tor have suggested having micropayments, such as the X-Pay system, that uses blind signatures to have users pay for bandwidth, or the TEARS and Torcoin systems that reward relays themselves with some sort of payment for proof-of-bandwidth. However, none of these systems have worked due to an inability for users to engage with micropayments. In general, these systems have the same essential design, descending from the original work by Chaum on blind signature-based payments for anonymous e-cash with a centralized bank, as demonstrated by the GNU Taler system. In contrast to these centralized efforts, there is tremendous interest in *decentralized* approaches to financial incentives with Bitcoin and Ethereum. None of the above privacy-enhanced systems have been deployed with any success, with the exception of Chaum's attempt to deploy anonymous e-cash via DigiCash, which went bankrupt. Another attempt to enable micropayments was the centralized e-Gold project, which was ended due to money transmitter regulations.

An ICO (Initial Coin Offering) is the use of blockchain technology to fund the creation of new technology by offering some "proof of stake" in the new technology by virtue of posession of

[4] https://www.ietf.org/meeting/upcoming.html

coins. In general, an ICO offers investors to buy some finite amount of tokens. These tokens are generally stored on a blockchain, and so are often considered a kind of "altcoin", a technology that creates a new kind of coin that is specialized for the technology being developed by the new venture. In general, the venture behind the new technology sells some amount of these tokens to pre-finance the development of the new technology via public sale (as well as possibly a private sale to accredited investors). Some amount of coin is not sold, and usually maintained by either the venture directly or generated via a decentralized proof-of-stake or proof-of-work mechanism. The key is that this token is released in some form of predictable schedule, similar to Bitcoin, and that the early investors get some kind of advantage by buying these tokens earlier. The main reason why the ICOs are successful is that, unlike Bitcoin, the Ethereum blockchain has a very straightforward specification language, that includes the "ERC20" smart contract for token specification, and allows ether to be converted into new customized tokens for a given ICO via a smart contract. Yet unlike the previous efforts to make anonymous e-cash, blockchain technologies (with the exception of Moneoro and ZCash) are by design transparent and offer no privacy. This is because the amount of investing and transfer of funds is stored as global public knowledge in a blockchain.

For example, the Brave Browser created the Basic Attention Token (BAT) for micropayments for Web content and the Bancor Network created "Connector" tokens that allow conversion between Ethereum and other alt-coins according to a smart contract. These ICOs have raised a large amount of funds, with Brave (one of the first ICOs) raising over 35 million USD in June 2017 and Bancor raising even more, 153 million euros in July 2017. ICOs have continued and are now happening at a rate of over 100-200 a month, although unlike the early ICOs they raise significantly less. Still, the amount of funding in ICOs currently overwhelms the amount of funding for venture capital. However, as regulations set in and a number of "scam" ICOs have appeared, investors have become increasingly skeptical and the amount of funds raised by ICOs now typically runs between 10 and 20 million euros. However, due to the strong market performance of both Bitcoin and Ethereum, the ICO investing market is still strong. One advantage of the Bitcoin ecosystem is that there is a large amount of investors already in the system, unlike other micropayment systems. Ethereum, unlike Bitcoin, has been designed to pay for the development of software via payment for running replicated smart contract code. This is done via the conversion of ether, the token used on the Ethereum blockchain that requires mining, to "gas", which is the measure of the computational requirements of a given transaction based on the Ethereum virtual machine (EVM) operations required to execute the smart contract. It is also trivial via services such as Coinbase[5] to convert bitcoin to ether. With ether in hand, investors are then capable of running the ERC20 smart contract to convert their ether to the token. The ether then goes to the new venture, who may convert it to fiat currency in order to fund the further development their enterprise.

In general, ICOs are a new legal instrument for fund-raising and thus the regulatory angle of them is still very much under development. In general, there is concern that an ICO is a form of *security*, which is defined using the "Howie" test by the United States Securities Commission, i.e. a form of equity in "common enterprise" where the profits of holders of equity are bound to the profitability of the company. Although Singapore has set up a "financial sandbox", the USA has sent mixed signals and so it would better to create a utility token that is clearly not a security due to its value for privacy-enhancing technologies in solving an outstanding technical problem. One problem we hope to solve is anonymous authentication, which is needed for some high-risk users that want one-time accounts for whistle-blowing and corporate users that wish to keep private their phone number and other personal data from the service provider.

Luckily, some jurisdictions have clear laws over utility tokens and ICOs. We would prefer the regulatory approach based on European law that is in full compliance with the same environment as the GDPR. In this regard, at the present time, the most advanced regulation in terms of ICOs is

[5] https://www.coinbase.com

currently in Switzerland. The Swiss Financial Market Supervisory Authority (FINMA) works with the lawyer of the organisation hosting the ICO to determine whether or not the organisation's ICO functions as a utility token or as a security. An organisation, legally incorporated in Switzerland, is required as the smart contract specification (including an ERC20 contract) is considered an asset, and so this asset must belong to either a Swiss Foundation or a Swiss AG. FINMA does this by viewing a whitepaper and making a legal judgement, and this legal judgement is required before the public sale of the ICO. Therefore, if PANORAMIX is to take advantage of a tokenized economy, it would need to partner with an existing Swiss organization or create a new one.

2.3.2 Privacycoin ICO Concept

In order for the ICO to succeed a wider alignment between stakeholders and service providers should take place. PANORAMIX consortium members aspire to play a leadership role in its development. Nevertheless, all plans reported for now are tentative and depend on advice from FINMA, consultants, and lawyers. The general idea is as follows: The ICO proposes to create a utility token, tentatively called *privacycoin* that will serve as an access tokens that allow privacy-enhancing technologies to be paid without knowing the identity of their users; this in particular will include Panoramix members but it will be readily expandable to more partners. We believe that investment into privacy enhancing technologies through this organisation, and its network of experts, will be able to address fundamental problems by helping fund many projects in the area beyond PANORAMIX such as the Greenhost VPN or the Riseup ecosystem and others. The integration of the Panoramix framework to use cases beyond the project (such as e.g., Riseup incorporating metadata resistance based on Panoramix software) are currently lacking a way to monetise the core open source infrastructure of their services and hence facilitate the expansion of their code base.

The general plan is to create a privacy-enhanced identity eco-system, where there will be an ICO sale to buy tokens that can be redeemed in a decentralized network of privacy-enhanced technologies. In essence, we will be creating an anonymized Facebook Connect. This eco-system will allow *Service Providers (SPs)*, such as Panoramix and even third-party VPNs and messaging providers, to authenticate users without knowing user identities via an *Identity Provider (IdP)*. In addition, this system allows the Service Providers get paid for services indirectly by users via their interactions with the IdP, and for the SPs to report abuse to the IdPs without using a centralised blacklist. The system will have two kinds of tokens: The first token is a *privacycoin* (PC) which is generically minted from an ERC20 contract, and these privacycoins can be exchanged for anonymous access credentials (ACred).

To overview the system, anonymous access credential will use a signature scheme with re-randomisation, allowing different uses of the credential to not be linked (and so preserving privacy). These credentials are *generic* and can be used to authenticate users in a privacy-preserving way to any service providers. These anonymous credentials can be obtained via exchanging privacycoins. The amount of privacycoins is linked to the capacity of the system using a proof-of-stake system. Thus, as more service providers, such as more mix nodes in Panoramix or more Panoramix-enabled applications, join the tokenised privacy-enhanced ecosystem, more PCs can be minted. However, they will be printed in a deflationary and predictable manner, as to encourage their purchase by users and investment in the early stages of the growth of privacy-enhanced eco-system. There will be a market of IdPs that will provide different levels and kinds of authentication.

A blockchain then creates and distributes PCs to a set of SPs and possibly other services. The IdPs mediate the authentication of users and the distribution of ACreds to users in exchange for PCs. Thanks to IdPs being ran by separate entities, SPs such as mix-net nodes do not have to maintain a payment infrastructure or authentication infrastructure. The users in turn pay the IdPs for the ACreds with PCs. These ACreds are redeemed to access the network in a privacy-enhanced and unlinkable manner, although schemes such as Hidden IBS (Hidden

Identity-Based Signatures) allow some identifying information, such as an email address, to be encrypted into the re-randomizable ciphertext of the ACred. Therefore, if an anonymous user commits some act of abuse, it can be reported from the service provider to the identity provider, who under the correct conditions can de-anonymize the users by decrypting the information in the ACred.

The entire token ecosystem works in epochs or rounds, similar to Tor: In each round, an IdP commits to adding resources to the network (bandwidth, money, etc.) and each SP also presents their costs (bandwith, server space, etc.) in terms of capacity to the proof-of-stake system. These commitments are recorded on a blockchain. The blockchain mints PCs in accordance with the available resources it is contributing to the network. At the end of each round, the SP can report any abuse about users from a particular IdP as well as how much of its resources were used. The IdPs have a "smart contract" to pay the SPs for their users who accessed the network. At the end of each round, account balances between the IdPs and the SPs are settled when SPs print to the blockchain how many ACreds they have received per IdP and the IdPs then transfer the SPs the PC to compensate them, and a new round commences. Whether or not an IdP paid or was abusive is recorded in a public but permissioned blockchain shared between all IdPs and SPs, who then can use the reports to either accept or not accept tokens from particular IdPs. Thus, IdPs are incentivized to both charge their users, pay SPs, and prevent abuse. The ecosystem is expandable and upgradable, which would allow other applications such as e-voting to share a generic tokenized infrastructure that could support any privacy-enhanced technology using core infrastructure of service providers, such as mixing nodes.

The ICO itself would allow the selling of these PCs for ether using a standard ERC20 contract. This ICO would fund the development work. However, the system is not envisioned as actually using Ethereum outside the ICO. The token pre-sale would allow the early buyers to have tokens that match the available resources in the eco-system at the time of its launch. The timing and price of the ICO will be determined in consultation between the regulatory authorities of FINMA and the independent Swiss organization (which may or may not adopt Panoramix), and financial and legal experts in ICOs.

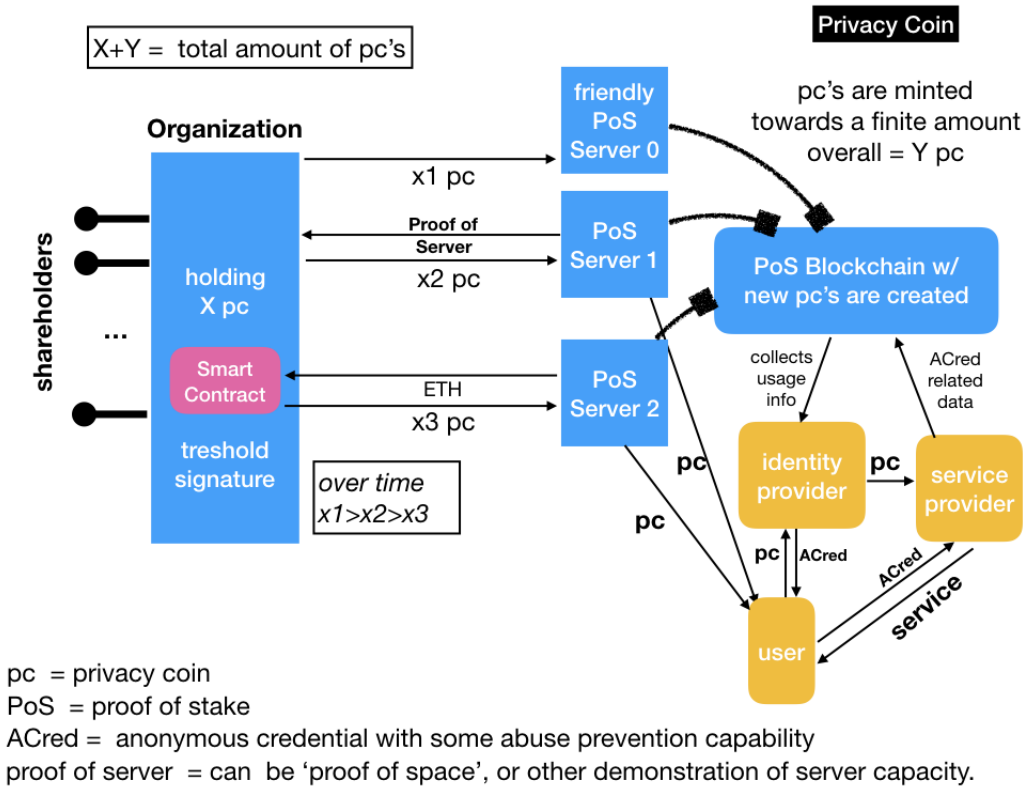

Figure 2.1: A graphical illustration of the tokenised system and the ICO. The initial ICO system provides stake either directly to "friendly" servers, (that are part of the system's inception), servers that provide a proof of server and servers that provide funding via an Ethereum smart contract. Subsequently, the PoS servers engage in the maintenance of the PoS blockchain that supports the ecosystem of Identity Providers, Service Providers and Users.

3. Individual Exploitation Plans

3.1 Overview

This chapter contains the individual exploitation plans by the project's partners. We first propose some general exploitation strategy advice in the following section that can serve as a guideline for the partners to formulate their individual exploitation plans. The partner-specific exploitation plans will follow in the subsequent sections 3.3 and 3.4.

3.2 Exploitation Strategy Guideline

The goal of exploitation in PANORAMIX is to ensure the sustainability of the project's results beyond the project end and to demonstrate how PANORAMIX has influenced the EU landscape. Exploitation includes multiple forms:

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.

We have compiled the two lists of general exploitation points as a prelude to each individual partner's exploitation strategy. We categorise these points in two broad approaches, one oriented towards the industrial partners and one addressing the academic partners.

3.2.1 Guideline for Industrial Partners

General strategy

- Focus on the main results from the project (products, services, ...) and their commercial viability.
- 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.

- Identify drivers for a successful exploitation and consider how those drivers can be harnessed and strengthened.
- If there are obstacles to a successful exploitation of the project from today's perspective, address them early on.
- Put a strong focus on how European stakeholders (customers of cloud services, providers of cloud services) can profit from the exploitation of the results.
- 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.
- Identify concrete customer needs that are addressed with the solution and product, and describe ways to quantitatively measure the success.
- Involve marketing, product-management, and sales departments early on in the process.
- If possible, start exploitation of intermediate results already during the project.
- Consider synergies for exploitation with other projects, possibly also funded ones.

Economic factors

- Aim at a quick access to the market. If necessary, create new markets for a successful exploitation.
- Address the market for exploitation today (market analysis, prognoses, technical developments).
- Assess the competition for the developed results, in Europe and worldwide.
- Provide innovation in project results, ensure there are advantages compared to competitors.

Scientific and technical goals

- Assess the impact of general technological progress on the exploitation scenarios.
- Pay attention to non-technical developments (legal aspects, privacy aspects, ...) and their influence on exploitation.

Intellectual property

- Consider to protect intellectual property, for example, through patents.

3.2.2 Guideline for Academic Partners

General strategy

- Identify drivers for a successful exploitation and consider how those drivers can be harnessed and strengthened.
- If there are obstacles to a successful exploitation of the project from today's perspective, address them early on.
- Put a strong focus on how European stakeholders (customers of cloud services, providers of cloud services) can profit from the exploitation of the results.

- 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.
- Identify concrete any student and staff needs that may be addressed with the solution and product.
- If possible, start exploitation of intermediate results already during the project.
- Consider synergies for exploitation with other projects, possibly also funded ones.

Scientific and technical goals

- Assess the impact of general technological progress on the exploitation scenarios.
- Pay attention to non-technical developments (legal aspects, privacy aspects, ...) and their influence on exploitation.
- Pay attention to the competition for the developed results, in Europe and worldwide.
- Provide innovation in project results, ensure there are advantages compared to competitors.

Intellectual property

- Consider to protect intellectual property, for example, through patents.

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.
- 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.
- The project should help to attract new researchers and students.
- Engage in improved dissemination activities through the project, for presenting work in conferences (industrial and academic), journals, and so on.
- Explore new scientific communities or try to get into other, relevant communities.

Sustainability

- Make the results of the work available as open-source.
- Contribute results to established open-source projects.
- Invest in maintaining the project results after the project ended.
- Plan follow-up projects the build on the results.
- Form new relations during the duration of the project and engage with new partners in future collaborations.
- Exploit the project for acquiring new projects and further funding.

Technology transfer

- Trigger interest in the industry for your project results.
- Ensure that students gain valuable knowledge by their work in the project, which they will take to industry.

3.3 Exploitation Plans from Academic Partners

In this section, the project's academic partners present their individual exploitation plans. This typically includes the offering of courses and seminars with topics related to the project. Through that, they can attract researchers and new students to work on and improve the ideas of the project.

Another area of focus for the academic partners within PANORAMIX is the exploitation of their work and project results through contributions to open-source software, particularly the PANORAMIX mix-net framework as major outcome of the project. Its maintenance presents an equally important objective to ensure that the results of PANORAMIX will remain available and relevant long after the project terminates. This can be supported by building and engaging a developer community around PANORAMIX.

The PANORAMIX software and the community that we anticipate to build around the framework will form a foundation for further research and development in the area of privacy preserving IT services. The availability of the PANORAMIX framework and API is expected to be a valuable asset for all academic partners in terms of building new partnerships, engaging in future projects and acquiring further funding at the national and EU level.

3.3.1 Exploitation Plan 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 Plan of Partner UCL

UCL is a non-profit educational and research organisation and in line with its aims does not aim to generate profit. However, the PANORAMIX outcomes, particularly those leading to high-quality and high-impact publications by UCL staff will be considered for submission to the UK Research Excellence Framework in 2020, i.a., "The Loopix Anonymity System" research paper funded by PANORAMIX is a 4-star Research Excellence Framework submission for UCL.

On the basis of this assessment, the UK government allocates research funding to UK research departments, and as such contributes to the economic viability of UCL. Moreover, participating in such an important project as PANORAMIX helps to obtain next EU funding.

Work in PANORAMIX is actively contributing to increasing UCL's capacity around two key areas:

(1) privacy-enhancing technologies relating to cryptographic and networking technologies, and

(2) privacy-enhancing technologies relating to statistical techniques and machine learning.

This capacity, and the track record of excellence will be used in the future for accessing a number of funding opportunities: further grants on requiring expertise on those topics, as well as maintaining UCL's status as an Academic Centre of Excellence in Cyber Security beyond 2016.

UCL's expertise in Privacy Enhancing Technologies and the PANORAMIX project already allowed us to obtain a new funding for the EU H2020 DECODE project. Moreover, in 2017 the ACE status for UCL was renewed and the PANORAMIX project contributed significantly to this success.

Thanks to the involvement into PANORAMIX project and privacy-enhancing technologies UCL is also now a Center for cybersecurity teaching excellence. Resources associated with PANORAMIX are already being supplemented by other grants (from the EPSRC) to deliver better solutions and analysis.

PANORAMIX employs two full-time doctoral students, Ania Piotrowska and Vasilis Mavroudis, and the outcomes from PANORAMIX will directly contribute to their doctoral training, and ultimately to the successful completion of their Doctoral thesis on the topics of efficient mix networks and private statistics. PANORAMIX employs also a post-doc, Dr. Sebastian Meiser, whose work will be a great contribution for academic and industrial partners involved in the projects on cryptography, security and privacy.

In terms of Masters-level research, PANORAMIX is very related to the *Privacy Enhancing Technologies* course (COMPGA17 at UCL) taught by Prof. Danezis, and outcomes may be integrated as exercises or techniques into this course. For exploitation purposes, UCL proposes a number of PANORAMIX-related topics for Masters' theses. Currently, Ania Piotrowska and Prof. George Danezis co-supervise an MSc project (Summer Term 2017) focused on building an

anonymous communication system based of mix networks. This project incorporates elements of the solutions and development ideas proposed by the PANORAMIX project.

UCL maintains a number of influential Privacy and Security themed blogs, from our collectible blog *Bentham's Gaze*[1] to individual staff blogs such as *Conspicuous Chatter*[2]. We plan on using the outcomes of PANORAMIX and the expertise gained to increase the research group and institution prestige by disseminating those results through those platforms as well as twitter.

UCL also maintains a number of open source projects of close relevance to PANORAMIX, such as the petlib cryptographic library[3]. PANORAMIX results will be integrated into the library, and other standalone projects, such as mix-net components or systems for private statistics are going to be made available through open source code repositories under a permissive license. The UCL code repositories, already including PANORAMIX related components, are at https://github.com/UCL-InfoSec. UCL is also involved in the PANORAMIX system design team and writing of the PANORAMIX system specification. The open-source specification allows sharing information about the design of the PANORAMIX system and gives the opportunity for other members of the community and industry to develop the ideas proposed by the PANORAMIX project for their own use.

3.3.3 Exploitation Plan of Partner UT

The Cryptography Research Group at the University of Tartu is well known for its (non-profit) engagement in providing theoretical backgrounds for secure e-voting schemes and mix-nets. Over the recent years, the group has proposed a number of papers analyzing security of various e-voting schemes, as well as published new secure, private, and efficient schemes for shuffling arguments that lay at the bottom of every mix-net and that are usually their efficiency bottleneck.

UT calls the exploitation successful if the cryptographic tools that the group provides meet a software implementation. This can be achieved in several ways, like an implementation of a shuffle argument as part of a mix-net used to protect voters' privacy in e-elections, or an implementation of delivered tools as a part of an application providing anonymous messaging and/or surveying. UT will try to reach this goal by cooperating closely with industry partners who are either inside or outside of the PANORAMIX consortium.

Moreover, UT calls the exploitation successful also if it manages to create an academic community focused on mix-net research. This goal is pursued by organising meetings and seminars addressed to computer science students and young researchers. UT also shares PANORAMIX ideas by taking part in various workshops (e.g, summer schools) that gather PhD students from a number of universities.

Scientific and technical goals For now (July 2017) the most efficient shuffle arguments in the common reference string model have been proposed by the University of Tartu. However, it has to be taken into consideration the possibility that some other, independent research group provides a more efficient and robust argument. In this case exploitation plan will be endangered since developers would rather choose their argument over an argument provided by the University of Tartu. On the other hand, it has to be mentioned that University of Tartu has several advantages over competitors like:

- world-class experience in theoretical aspects of mix-nets,
- a group of researchers focused solely on mix-nets, and
- constant access to practitioners and developers of e-voting systems.

[1] https://www.benthamsgaze.org/
[2] https://conspicuouschatter.wordpress.com/
[3] https://github.com/gdanezis/petlib

Intellectual property Output of the research will be patent-free and freely available, e.g. via the *Cryptology ePrint Archive*[4] of the International Association for Cryptologic Research (IACR). This online database is used by many cryptographers and security experts as a primary source of knowledge on recent cryptographic development.

Academic impact and education During the project a number of seminars will take place. UT conducts weekly seminars that are addressed to both Master's and PhD students and cover topics relevant to mix-nets. These seminars are open and also host researchers and industry representatives involved in independent research and software development on e-voting.

For exploitation purposes UT will propose a number of PANORAMIX-related topics for Masters' and Bachelors' theses. UT believes that passing and explaining ideas behind PANORAMIX to younger students will secure the future development of the project and increase the awareness of PANORAMIX goals. The group will also share the knowledge about mix-nets outside the University of Tartu by giving lectures and seminars in other academic centres.

Sustainability Since mix-nets are (usually) important building block to provide functionalities like secure, anonymous and verifiable electronic voting or anonymous messaging in the Internet, UT believes that research on mix-nets will be of great interest for the computer security community. The group expects that there will be a noticeable demand on the knowledge possessed by it during the project. UT will be participating actively in sharing the awareness of the project in the security experts community.

All research output produced at UT as part of PANORAMIX is available openly on the Internet. To provide sustainability of the research even beyond the timeline of PANORAMIX, the University of Tartu often meets with e-voting-focused industry representatives, for instance from TIVI[5], transferring know-how and spreading the idea of the project. UT also reaches out to young researchers transferring project know-how and research results.

UT believes that participating in such an important project as PANORAMIX will be helpful in reaching follow-up fundings. These will assure that mix-net research can continue even beyond the project's time span.

Technology transfer Despite of providing theoretical background to secure mix-nets, the University of Tartu will offer consulting services to those who would like to implement shuffle arguments obtained during the project.

The University of Tartu provides stipends for a number of PhD students and post-docs involved in PANORAMIX. When the project ends, these people will be a valuable asset for any academic or industrial organization demanding high-level knowledge on cryptography and security of mix-nets, especially if used to provide anonymity on the Internet or for secure e-voting.

3.3.4 Exploitation Plan of Partner KUL

KU Leuven expects to exploit the outcomes of the project by promoting their use within established communities. Our main aim is to enable technology transfer to existing communications networks that provide privacy and security properties. We primarily target the Tor network due to our working relationship with the core development team, although we are exploring other networks as well.

Tor is an anonymous communications network providing strong privacy and security guarantees. Its user-base count is approximately 2 million making it one of the largest networks with these properties. However, it lacks defenses (by design) against global passive adversaries, i.e. observers for whom both ingress and egress traffic is visible. mix networks provide a natural

[4] https://eprint.iacr.org/
[5] https://tivi.io/

remedy for this shortcoming, and Panoramix in particular will provide a compelling working codebase, in contrast to earlier mix-net proposals that lacked this key element to adoption. Furthermore, we are also working on encouraging the use of privacy-preserving statistics collection, with the Tor network, a heretofore unacceptable practice – due to risks to end-user privacy and operator security. Steps have been taken by founding and serving as a member of the ethics board of the Tor project. Our aim as a member is to place an emphasis on safely collecting data on the Tor network, both for Tor's own operational usage, and those of researchers wishing to run experiments on the live network. This promotes the need for the research results from WP 6.

A consequence of this emphasis on private-statistics collection has generated interest within the research community to progress the state-of-the-art in this area, with at least one project, at the Naval Research Laboratory, investing heavily in the engineering of private-statistics collection easy to use and deploy. The project can benefit from this push in the state-of-the-art since the results of this engineering effort are open-sourced and licensed according to the same legal regime as the one the project uses.

We are also aware of other contemporary research activity around mix networks such as Vuvuzela, Alpenhorn, and cMix. These proposals are the current state-of-the-art with respect to scalability, robustness and latency; however, they do not represent significant advances in terms of deployability and accessibility. It will be our aim to leverage research findings from these proposals to further enhance our own product.

With regards to our educational activities, Panoramix will provide new topics and new motivations to the *Privacy Technologies* course, taught by Prof. Diaz. The aim to make Panoramix widely used, and the techniques that both the academic and the industry partners will research to solve real world problems, will increase the interest of potential new researchers in the project. From the academic year 2017-2018, the *Privacy Technologies* course will introduce several of the research topics that Panoramix tackles, effectively updating the material that elaborate on mix networks as a solution to problems requiring anonymity.

3.4 Exploitation Plans from Industrial Partners

The industrial partners' exploitation objectives mainly focus on the three use-cases e-voting, survey data collection and messaging. These aim at exploiting the applications of the mix-net, thus providing a further incentive to maintain the basic software and infrastructure. All the proposed use-cases have direct commercial value and can be evolved into market offerings by the individual use-case participants. The different use-cases provide different strands and if some are met by organizational obstacles, others can still thrive into successful commercial products. Hence, we aim at leveraging the basic mix-net software and infrastructure in all of them, but aim at little overlap or integration between the use-cases in order to not prevent the success of one by another. It is the individual partners' responsibility to drive and market the results of PANORAMIX.

3.4.1 Exploitation Plan of Partner GRNET

GRNET has developed the Zeus open source e-voting system (see http://zeus.grnet.gr), which has been in operation for several years. Hundreds of elections have been held to date, involving hundreds of thousands of voters. To date, Zeus has been used, for instance, in all the universities in Greece, and in the private sector at the Hellenic Chamber of Hotels[6] and the Association of Greek Valuers[7]. GRNET is committed to further development of Zeus and PANORAMIX will play an instrumental role in the evolution of Zeus.

[6] http://www.grhotels.gr/EN
[7] http://www.avag.gr/

In particular, Zeus guarantees voter anonymity via mix-nets, currently employing a traditional Sako-Kilian mix-net. Although there are no problems from a security perspective, Sako-Kilian mix-nets are slow, as they perform a large number of shadow mixes in order to thwart adversaries. In practice that means that Zeus can decrypt and anonymize a few thousands of ballots in a matter of hours, running on a single, yet capable server machine (16 2.2 GHz Intel CPUs, 10GB RAM). One way to speed up the process would be to throw more computing power at the problem, as the Sako-Kilian mix-net can be easily pararellized. It is much more desirable, however, to have a faster mix-net to begin with.

There exist a number of other mix-net solutions apart from Sako-Kilian, but most of them are covered by patents and are therefore unusable by an open source project. In addition to validating other open solutions, GRNET is keen to leverage the mix-net technology that will be produced by PANORAMIX by incorporating it directly in its production Zeus service.

The aim of GRNET is to be able to hold elections for hundreds of thousands, or even millions of users, without having recourse to expensive hardware, while producing the election results in minutes. This will greatly improve the user experience in the elections that can already take place in Zeus, while opening the door for elections on a much larger scale. Moreover, this will allow us to offer a much more economical solution with lower hardware and operating costs.

The mixing infrastructure that we are developing will have Zeus as one particular use-case. However, all the code we write is open source (see section 2.2), so it will be usable by other systems as well.

Apart from elections, the technology behind Zeus can be used for other anonymizing purposes. Indeed, it has already been used as a means for conducting anonymized surveys. Although it is capable to run surveys of a few thousands of users in a reasonable amount of time, a new, faster mix-net will allow much larger surveys that cannot be carried out by traditional means. Apart from the cost reduction, Zeus may help in reducing bias in survey responses by providing strong anonymity guarantees to respondents.

Furthermore, the mix-net infrastructure developed by GRNET is not limited to re-encryption mix-nets, which are typical in elections. The design and architecture of the mix-net infrastructure can also accommodate decryption mix-nets, which are typical in messaging anonymisation (for instance, Tor). GRNET will ensure that the mix-net infrastructure is usable separately from Zeus, as a generic platform for anonymization purposes, including messaging. GRNET will therefore make the mix-net infrastructure available as a separate, independent software product, under an open source license.

3.4.2 Exploitation Plan 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, 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 is 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.
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 are going to apply the following approach:

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

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

While we can 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, we are going to implement the above approach and demonstrate the use and advantages of the Panoramix mix network in a collaborative (SaaS) application (WP6). We collect data (e.g. survey answers, sensor data from IoT devices) 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 WP6 is to equip the database with the necessary mechanisms and connect it to the mix network. In the process, we will gain hands-on experience on employing mix-nets and differential privacy, which will be beneficial 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 will mainly absorb the results from WP3, where SAP is 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 expected results of SAP's research efforts within PANORAMIX will therefore directly feed 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 HANA (SAP's in-memory, column-store database) 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. Besides leading the research efforts, Dr. Florian Kerschbaum is the chief architect for the use of cryptography and is in direct contact with SAP's executive board and SAP customers to position anonymization as a differentiator for cloud adoption and data sharing. 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 is to create awareness in the development organization. We will participate 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 aim to spur demand and to disseminate our roadmap. We will involve decision makers and pilot customers in order to create a roadmap for the productization of PANORAMIX results.

In the third year, we initiate the technology transfer. We will create a detailed transfer plan and intend to hand over the developed code.

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 so far:

- 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 are planned and further collaboration is intended.
- 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 section 4.3.2).

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.

3.4.3 Exploitation Plan of Partner Greenhost

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. These customers also appreciate Greenhost's unique focus and branding around the use of sustainable energy in its hosting infrastructure. Greenhost has a stellar reputation for supporting human rights defenders for free (with costs being subsidized often by grants from human rights organizations such as the Open Technology Fund) as well as its paying customers and delivering contract. Customers include IESA Shift, Bits of Freedom, De Webcirkel, EvoSwitch and Free Press Unlimited. Thus, a good portion of the user-base of Greenhost, consisting of environmentally-aware activists and NGOs interested in digital rights, also have an interest in secure messaging powered by the PANORAMIX mix networking system.

There has been an explosion of interest in secure messaging (i.e. end-to-end encrypted between users) applications over the last year, with the adoption of secure messaging by WhatsApp (Facebook), Apple iMessage, and support in process for Facebook Messenger and Google Allo. However, there is no open-source and high-security secure messaging client that can be self-hosted and run by a company like Greenhost on commodity hardware. All secure messaging services, including fully open-source end-to-end encrypted messaging applications used by high-risk activists such as Signal, require the consumer completely trust the secure messaging provider, which is often a company in a different jurisdiction than the consumer (almost always the United States).

As shown by the Snowden revelations and the more recent FBI vs. Apple case, even in the United States it is hard to trust a third-party to actually secure their applications. Open source is a requirement, but so is trusted hosting and even self-hosting for enterprise and high-risk activists. Furthermore, none of these encrypted messaging applications offer compatibility with existing open and federated e-mail systems, which are still dependent on encryption standards such as PGP and S/MIME that do not take into account the protection of metadata against powerful adversaries. Given that business and enterprise messaging is still dependent on email, it

makes sense to make secure messaging applications compatible with e-mail. Lastly and most importantly, none of these competing secure messaging algorithms provide any protection against attacks based on metadata, such as attacks by third-parties to de-anonymize the social network of users based on timing and size of message information. In these existing systems, the social network of a user is simply controlled by the trusted server, usually a company such as Google, Facebook, or Apple. There seems to be an opening for a product based on PANORAMIX that can offer real security including security against attacks on metadata. By hosting such a service in Europe, Greenhost would be the first secure messaging e-mail provider with a unique and superior technical solution in compliance with the new European General Data Protection Regulation.

Greenhost has chosen to adopt as its secure messaging platform the open-source LEAP codebase, the first and only high-security, open-source encrypted e-mail provider that can be completely self-hosted and also can work as a 'turn-key' solution on the server-side and the client-server. It would allow users to self-host on Greenhost's trusted virtual machines, as well as use an instance that would be run directly by Greenhost for ease-of-use. As this solution is completely open source, it can be hosted in European jurisdiction as well as altered to fit additional local regulatory conditions outside the General Data Protection Regulation, and users can be assured of its quality by inspecting the code and hosting an instance themselves. Although a user may want to host their own, in order to use mix networking multiple co-operating servers are necessary, and for these users simply working with Greenhost would be more appealing than self-hosting. As LEAP has gone through rigorous security auditing, providing higher security assurances than competing off-the-shelf secure messaging products at a lower cost, Greenhost can control the software and hardware as well as future development for Greenhost users. Therefore, Greenhost's exploitation plan consists of beta-testing the software with its current user-base, and then pivoting to see if other high-risk and enterprise customers would be interested in hosting their messaging either directly on Greenhost or using Greenhost virtual machines in order to take advantage of the PANORAMIX infrastructure.

Globally, the market size for secure messaging solutions and encrypted e-mail gateways was 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.[8] Given that the Greenhost user-base in beta is mostly in Europe, and that Europe will be moving to increased adoption of self-hosted open-source solutions and stronger regulations due to the new Data Protection requirement, we will focus on competing against American secure messaging and e-mail providers in Europe. Currently, the use of e-mail by Europeans in enterprise and NGOs who are not using Gmail is fractured between numerous small e-mail providers or self-hosting providers that constitute 25% of the market, and so the addressable market is estimated to be 500 million euros, so even capturing a relatively small percentage of that messaging/e-mail traffic could form the basis for a sustainable business for secure e-mail. E-mail is still a growth area, with a growth of 3%, despite concerns that it will be replaced by messaging software such as Slack for corporate use.[9] We believe approximately 50% of this market will need to change to a solution that is both higher security and is placed in a European jurisdiction due to the unification of various European data protection (privacy) regulations by the General Data Protection Regulation that was adopted in April 2016 and must be fully adopted by European states by the end of 2018. This is compounded by the fact that the European-America data-sharing "Safe Harbour" agreement was recently deemed illegal and its replacement "Privacy Shield" is still under development, but so far deemed not strong enough by European Union Data Protection regulators.

The general trend in Europe is to more self-hosting of data and tighter jurisdictional regulations so that messages that are locally hosted will become more critical for European enterprises. By

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

[9] http://radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

relying on beta-testing with end-user and word-of-mouth advertising from human rights activists, Greenhost hopes to expand its customer-base to the high-security enterprise market, with a focus on Dutch NGOs and SMEs as the 'go-to' market. While existing e-mail providers can also adopt the LEAP infrastructure and re-brand it, making market entry easier, Greenhost will be the first provider to offer PANORAMIX-enabled metadata protection that should provide protection against adversaries even as powerful as the NSA. PANORAMIX infrastructure provides a key distinguishing factor that should drive potential customers to Greenhost. We also have contacts in the European Parliament (such as Mattias Bjarnemalm) who would be interested in 'beta'-testing PANORAMIX-enabled messaging and interested contacts in firms such as Gemalto.

Greenhost uses open-source software and does not file patents. Thus, we expect to prefer Open Source Definition compatible licenses and not file any intellectual property claims related to PANORAMIX. Furthermore, with the help of our Advisory Board we will pursue a robust standardization strategy via the IETF and W3C, as these standards bodies have patent policies that encourage royalty-free licensing of patents. Although this is not a traditional business strategy, given that Greenhost relies on the trust of its customers and the ability of customers to potentially self-host the software, patents would only erode the trust of existing customers and provide a barrier for new customers.

Although the precise timing of the exploitation plan is dependent on software development, for the first year of PANORAMIX (September 2015-August 2016), Greenhost has been focused on providing the necessary requirements to other partners (including detailed analysis of e-mail data) for constructing the mix networking platform as well as doing necessary user-experience and scalability work in order to launch beta-testing of the LEAP-enabled client by the end of August 2016. User testing will continue over 2017 and scale up as the PANORAMIX mix networking infrastructure is deployed by Greenhost in conjunction with other LEAP-enabled providers. In 2018, this should provide enough detailed feedback to begin market exploitation by the end of the PANORAMIX testing, with detailed user feedback presented in a privacy-preserving manner in D7.3. Overall, Greenhost believes mix networking presents a unique innovation solution for European SMEs to regain the secure e-mail and messaging market from dominant American players, and the timing with the General Data Protection Regulation is ideal in order to capitalize on this market.

In the second year, we have 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 in countries such as Lebanon with at-risk human rights activists, and helped run demonstrations at CPDP. We plan to announce mix networking for beta-testing by the end of 2018, and we believe this will generate considerable interest and eventually revenue for GH.

3.4.4 Exploitation Plan of Partner CCT

The Center for the Cultivation of Technology (CCT) is a non-profit incubator for open-source projects, specializing on Human Rights technologies for secure and unrestricted communication. In the PANORAMIX consortium, one of our roles 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. This will not simply offer code, but deploy a functioning, user-tested and -adopted mix-net-based messaging system, a fully functioning product that can be further refined by the wider market. Compared to other products or partial solutions on the market, our messaging system will provide unparalleled security, the trust that can only be gained through open source software, and the added distinguishing factor of the European legal framework as project base, which currently compares particularly favorable to that of e.g. US-based companies. Our work in the area of secure messaging will also continue after PANORAMIX, and due to our involvement in various messaging related efforts, we are in a unique position to continue the integration at service providers, and grow the number of mix-net node operators, all serving the overarching

goal of providing both secure and user-friendly messaging.

As an illustrative example, in a very similar fashion, CCT is working with the Torservers.net group, a network of currently 22 non-profit organizations in 15 countries which successfully operate the majority of Tor exit infrastructure, as public infrastructure using grants and donations, and with Tor Project, Inc. as maintainer of the Tor software. We believe in order for a mix-net to be successful, it needs to go a similar route and become public infrastructure. Our employees and volunteers will leverage their expertise in community building and fundraising for both the open-source project as well as for the operation and deployment of the mix-net infrastructure in ongoing partnerships with hosting and e-mail providers like Greenhost. We have already facilitated joint meetings with the Tor Project and the Panoramix consortium as part of our exploitation activity for PANORAMIX. We will continue to maintain these relationships and use PANORAMIX to gain a higher profile as a provider of mix networking infrastructure support.

Therefore, we can expect that in the future, to build and maintain a similarly stable, strong and secure public infrastructure, mix-net users and messaging providers will donate funds for the use of the mix networking infrastructure for messaging, as well as donate bandwidth to CCT to increase the throughput of the infrastructure. After the end of the PANORAMIX project, we expect this infrastructure to be self-supporting and sustainable financially.

4. Business Models

4.1 Overview

This chapter contains the business models for the PANORAMIX project's three use-cases. The main purpose of this chapter is to present the business models best suited to project partners, through which the generated innovation will be brought to the market. In the next section, a generic business model template that follows the Business Model Canvas approach[1], is presented.

4.2 Business Model Canvas template

Business Model Canvas is a strategic management template for developing new or documenting existing business models. It is a visual chart with elements describing a firm's or product's value proposition, infrastructure, customers, and finances. It assists firms in aligning their activities by illustrating potential trade-offs. All the elements included in Business Model Canvas can be seen in Fig. 4.1[2].

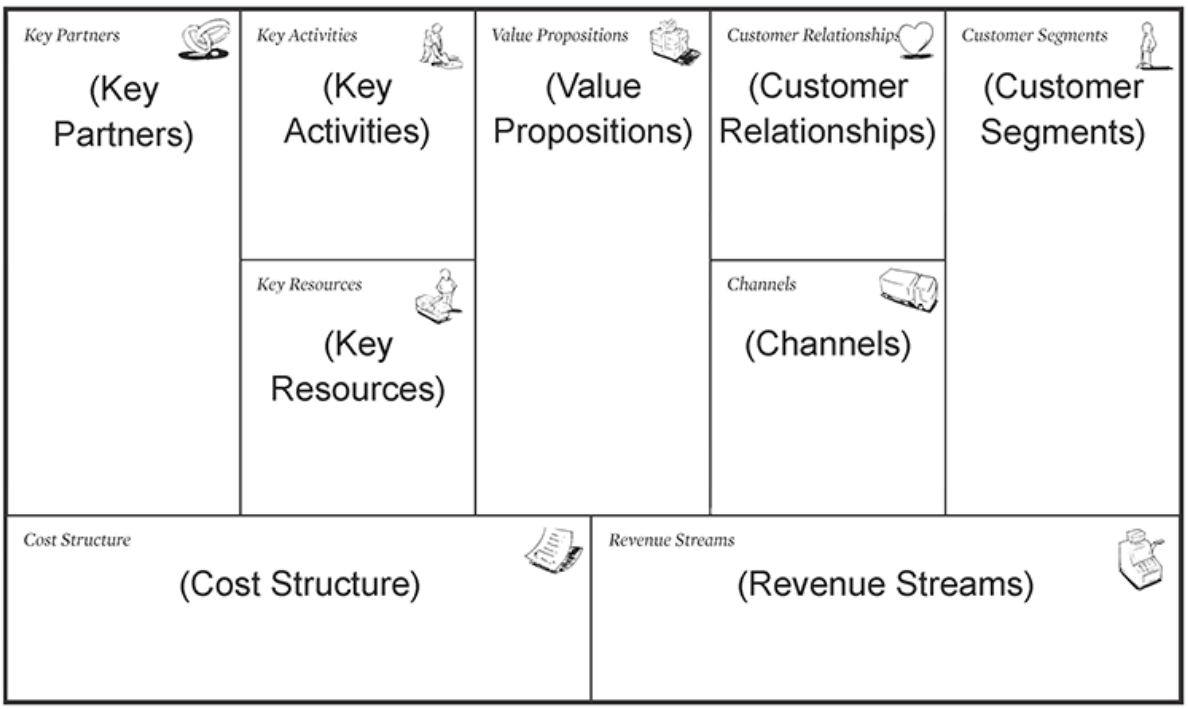

Figure 4.1: The nine elements of the Business Model Canvas

A business model that follows the Business Model Canvas approach must provide information on

[1]Wikipedia: Business Model Canvas, https://en.wikipedia.org/wiki/Business_Model_Canvas
[2]Image from https://www.alexandercowan.com/business-model-canvas-templates/

the following elements:

Customer Segments To build an effective business model, an organization must identify which customers it tries to serve. Various sets of customers can be segmented based on the different needs and attributes to ensure appropriate implementation of corporate strategy meets the characteristics of selected group of clients.

Value Propositions The products and/or services the organization offers in order to meet the needs of its customers. A company's value proposition is what distinguishes itself from its competitors.

Channels An organization can deliver its value proposition to its customers through different channels. Effective channels will distribute the value proposition in ways that are fast, efficient and cost effective.

Customer Relationships To ensure the survival and success of any business, organization must identify the type of relationship they want to create with their customer segments. For example, the way a customer interacts with the organization through the sales and product lifecycle.

Revenue Streams The way the organization makes income from each customer segment. For example, subscription fees or licensing, etc.

Key Activities The most important activities in executing the organization's value proposition. For example, for a product-driven business, this includes ongoing learning about new techniques to build better product.

Key Resources The resources that are necessary to create value for the customer. They are considered assets to a company, which are needed in order to sustain and support the business. These resources could be human, financial, physical and intellectual.

Key Partnerships In order to optimize operations and reduce risks of a business model, organizations usually cultivate buyer-supplier relationships so they can focus on their core activity. Complementary business alliances also can be considered through joint ventures, strategic alliances between competitors or non-competitors. For example, Key Partnerships with notes on their relationship to Key Activities.

Cost Structure This describes the most important monetary consequences while operating under different business models. For example, how do the Key Activities drive the costs.

In the following sections, business models for each use-case, which will be implemented in order to bring innovation to market, are presented.

4.3 Business Models for each Use-case

Each industrial partner is associated with a specific use-case/application which exploits the project's results. GRNET's business model focuses on e-voting, SAP's business model focuses on privacy-friendly surveying, statistics and big data gathering applications and GH/CCT's business model focuses on messaging applications. The academic partners in PANORAMIX all contribute where appropriate to the project's results which are further exploited in various ways by the industrial partners. In this section, business models per use-case are presented.

4.3.1 Business Model of E-voting Use-case: GRNET

GRNET provides Internet connectivity, high-quality e-Infrastructures and advanced services to the Greek Educational, Academic and Research community, aiming at minimizing the digital divide and at ensuring equal participation of its members in the global Society of Knowledge. Additionally, GRNET develops digital applications that ensure resource optimization for the Greek state, modernize public functional structures and procedures, and introduce new models of cooperation between public bodies, research and education communities, citizens and businesses.

ZEUS is an e-voting service provided by GRNET, that is executed on the ∼okeanos platform. The ∼okeanos offers computation, and storage clouds to the various GRNET customers. The objective is to provide an e-voting service supporting robust and verifiable private elections that scale up to 100K-1M ballots.

GRNET operates under the auspices of the Greek General Secretariat for Research and Technology / Ministry of Education, Research and Religious Affairs. GRNET has standard users coming from Greek universities, laboratories and the academic community in general. Furthermore, as a state institution it does not aim to compete or have any advantage against other companies that provide similar services. Hence, the presented canvas is not a standard lean canvas per se, and it has been adapted for the context in which GRNET operates.

Customer Segments. GRNET customers are mainly the Greek Academia, comprising from the Universities and the Research Centres. However, there are Public and Private Organizations that seek for GRNET guidance and services in specialized issues, like scalable e-voting services.

Value Propositions. GRNET's cloud infrastructure (∼okeanos) has been serving customers long before the start of the PANORAMIX project. It employs more than two thousand servers and supports more than thirty-one thousand virtual machines. Hence, being one step ahead, GRNET can incorporate the PANORAMIX mix-net technologies faster in its e-voting services and will be able to provide e-voting services able to support robust and verifiable private elections that scale up to 100K-1M ballots. GRNET will also provide e-voting preparation consulting services to interested organizations.

Channels. The usual channels for promoting the e-voting services and products, are GRNET's web site and main stream social media. However, since e-voting solutions are a relative sensitive issue for organizations and most of them hesitate to make the necessary steps in adopting corresponding solutions/services, GRNET will organize specialized workshops to inform interested organizations regarding our advance services.

Customer Relationships. GRNET is under re-organization concerning the specific part of its business. GRNET tries to redefine the business section that handles all customer relationships. The resulting schema, which will include helpdesk operations, will also include a specialized service delivery manager responsible for interacting with all the respective customers.

Revenue Streams. Typically, GRNET's services are subsidized. However, there are specific cases where GRNET provides a pay-per-service support stream. This essentially means that, most times, GRNET provides its services to its customers (members of the Greek Research and Academic community) for free. However, when other organizations of public interest request for its e-voting services, GRNET is obliged to provide them. In this case though, GRNET charges only the necessary costs (server time and support team effort). The PANORAMIX ICO detailed in Section 2.3 will be also considered as part of a long term strategy of expanding the availability of GRNET privacy enhanced services to its customers (who, possibly taking advantage of the ICO can provide payment in tokenised form).

Key Activities. Usually, the organizations that are in need of GRNET e-voting services, come from a physical voting past, making the transition a relatively demanding process. GRNET will invest in acquiring the necessary expertise needed to help organizations overcome all the obstacles preventing them to adopt the e-voting culture. This includes the ability to advertise successful experiences of other similar organizations to prospective customers.

Key Resources. The e-voting service, that will be efficiently delivered by GRNET, is based on the following key resources: GRNET's cloud infrastructure (∼okeanos) and the respective technology and business experts needed to handle all the necessary aspects of the provided service. GRNET successfully operates its cloud infrastructure. However, additional personnel will be needed to strengthen the technology and business staff, when the e-voting service delivery business grows significantly.

Key Partnerships. Other than the technology and framework that is being developed in PANORAMIX project, there is no other partnership needed in order for GRNET to provide its e-voting service to potential customers.

Cost structure. When the e-voting solution is ready for the market, GRNET's main costs will mainly consist of human resources and service hosting. The cost more specifically is based on the type and number of servers needed to successfully implement an complete e-voting session, as well as the respective personnel needed to support each e-voting session.

4.3.2 Business Model of Statistics Use-case: SAP

As a company transitioning its data and business operations into the cloud, our primary goal is to offer the outcomes of PANORAMIX through a cloud service business model. Therefore, we intend to provide the Panoramix mix-net and our differential privacy mechanisms in the form of a service-based solution that can be used by a wide range of customers, as outlined in section 3.4.2.

Customer Segments. Our customers are product and data owners from other development units within SAP. The primary customer segment is concerned with Internet of Things (IoT) business cases, where potentially sensitive data has to be gathered from many devices. Other important segments include human resources (HR) and support, cf. our list of exploitation activities and stakeholders in section 3.4.2. These business cases commonly involve collecting and processing personally identifiable information (PII) and hence require technical measures to protect the privacy of the data subjects.

Value Propositions. Big data and trends such as IoT have boosted both the demand and supply of data. While solutions to process and monetize this tidal wave of data have already been developed, the need to protect personal or sensitive data often prevents its utilization.

PANORAMIX technology therefore serves as a business-enabler in many of our stakeholders' business cases: While the Panoramix mix-net provides anonymity on the network level, differential privacy provides data confidentiality to prevent re-identification attacks. The proposed value hence consists of providing our customers a flexible anonymization cloud service combining the two state-of-the-art technologies to enable end-to-end privacy on both the network and data levels.

Channels. As detailed in our exploitation plan in section 3.4.2, we already have contacted and involved several stakeholders from various segments including IoT and HR. Furthermore, we continue our efforts to raise awareness of PANORAMIX within SAP, for instance by presenting our results at events such as SAP d-kom and SAP Security Summit.

Customer Relationships. Our business model strives to maintain customer relationships by a hybrid of self service functionalities and a community platform. Customers interact directly with the API to realize anonymization for their scenarios. The API is not specifically tailored. When facing issues or questions in respect to the API customers can interact with the community platform. The community platform is represented by a forum in which scenario specific questions can be asked and discussed with us as the service providers as well as other users. Consequently we envision the community platform as a basis for discussion of further development and adaptation requests.

Revenue Streams. Our business model is based on two revenue streams. First, in the case of central anonymization through the cloud service API recurring *usage fee* revenues are realized by charging customers depending to their data volume exchanged with the cloud anonymization. effectively resulting in a pay-as-you-go business model (i.e., based on data volume). Second, for the case of local anonymization in IoT (i.e., at the data source before sending data to the cloud, as depicting in our anonymization service) a *subscription fee* is collected in dependence to the number of sensors. An overview of our proposed pricing metrics is presented in table 4.1.

Component	**Privacy**	**Pricing Metrics**
Panoramix Mix-Net	Network-level	Network traffic (GB), Node hours (h)
Anonymization Service	Data-level (cloud)	Data volume (GB), no. of API calls (#)
Anonymization Service	Data-level (local[3])	Registered IoT devices (#)

Table 4.1: Summary of pricing metrics for anonymization services.

Key Activities. Our goal is to introduce state-of-the-art anonymization technologies to SAP, for instance by presenting our research in PANORAMIX and building prototypes to demonstrate these technologies to our stakeholders. Mix networks are one such technology, which provides anonymity to the communication partners when collecting sensitive data. Since the data itself is often sufficient to reveal its originator, we consider methods such as differential privacy to protect against reidentification. We focus our research activities on improving such mechanisms and adapting them to our applications.

Key Resources. Our envisioned business model relies on the cloud service at the core, realized through the SAP cloud building blocks (i.e., SAP Leonardo, SAP HANA Cloud Platform) as key resources for the service provisioning and integration with customers.

Key Partnerships. A key partner for SAP are the PANORAMIX consortium members that provide the mix network infrastructure, which is the main building block that provides anonymity at the network level.

Cost Structure. Due to their nature, mix networks are very resource intensive: Each message is routed through several peers, where many cryptographic operations have to be performed along their way from the sender to the receiver. Similarly, the anonymization service will be deployed on servers where resources must be provided to run the differential privacy mechanisms on the incoming data to be anonymized.

Consequently, our solution is provided as a cloud service that allows to dynamically scale the infrastructure to customer demand and minimize fix costs. This is reflected in our proposed cloud pricing model above, through which we aim at covering the costs and create a stream of revenue.

[3]Anonymization is performed *on-device*, that is, before data is collected or routed through the mix-net.

4.3.3 Business Model of Messaging Use-case: GH and CCT

CCT and GH provide secure messaging based on open source development, which faces unique obstacles and hindrances compared to larger and proprietary software development as well as unique advantages in terms of security and agility. Privacy and encryption technologies cannot fulfill their potential in proprietary form, where key components cannot be audited or improved by the community and so trusted by end-users. Actual long-term solutions for both citizens and enterprises rely on the expertise and openness provided by open source soft- and hardware are provided by GH in commercial form for end users, while CCT provides organizational support for open source developers themselves.

Customer segments. There are two distinct customer segments: The first is end-users of the Panoramix software, who will pay GH on a re-occurring basis for usage of the infrastructure. As outlined in D7.1, these users themselves include journalists, activists, and high-powered privacy-conscious corporate users. GH will via outreach to its existing customers in D7.3 determine which of these customer segments actually ends up taking up Panoramix messaging via GH.

The second customer segment is open source developers themselves and other deployers of the Panoramix mix-networking messaging system. The Center for the Cultivation of Technology (CCT) thus addresses this two-sided customer market by gearing its organizational services towards individual open source developers and projects, who can then concentrate on their core work of coding and developing, while CCT takes care of all related organizational, legal, and financial matters and so generates an income stream for itself. CCT plans to extend this customer segment to deal with enterprises and governments that will want to deploy the Panoramix mix networking messaging software.

Therefore, the development arm of CCT and GH targets the wider public of end users as well as enterprises, and develops and maintains open source technologies and products. It especially addresses organizations and institutions interested in cutting-edge privacy and encryption technologies, and provides respective products and solutions.

Value Propositions. The Panoramix mix-networking messaging system will present the first comprehensive privacy-enhanced messaging solution for both individual and enterprise use. Although other solutions may offer end-to-end encryption and resistance to local adversaries, Panoramix is the only solution that offers resistance to metadata analysis, including from the messaging server itself. Therefore, our solution will be both an attractive codebase for customers of GH wanting improved privacy as well as for open-source developers working on privacy-enhancing technologies who are looking for a generic anonymity network with a more powerful threat model than Tor.

Importantly, while GH will serve as the primary customer-facing entry to the Panoramix mix network, the Panoramix mix network has increasing privacy and security if different authorities control the mix nodes. The network also will have increased throughput and decreased latency with more nodes. Therefore, as CCT identifies and builds long-term relationships of individuals and companies in the privacy-enhancing technology space and takes care of organizational matters for the projects, including contract management, office and legal setup, organizational structuring, fundraising, progress reporting and tax filing, CCT can enable not only increased interaction between the Panoramix messaging codebase and software developers, but also as shown by CCT's work on `torsevers.net` in the context of the Tor network, but can also help interested non-profits, enterprises, and volunteers deploy and maintain mix nodes for the Panoramix messaging use-case.

CCT offers a one-stop solution for open source projects looking to either concentrate on coding or professionalizing their current organizational setup. While other partial solutions either demand the dedication of precious resources (especially time) or entail considerable financial burdens (for proprietary solutions and expensive services), CCT can take care of everything open source projects need, further provide help through expert advice and an invaluable network of

partner projects, and at the same time maintain its role as well-known, respected and trusted partner in open source circles. Providing such trusted, full-scale professional services is entirely unique in the open source development sector.

Similarly, CCT can provide to its institutional and business customers a cutting-edge open source technology solutions and services, combining the strengths of different partner projects whenever needed, and providing the level of business security that enterprises could not hope for when dealing with individual projects directly.

Channels. GH and CCT advertises its services on well-known open source portals and at similarly themed workshops and conferences (ranging from CPDP to RightsCon), in addition to its own website and social media channels. As much in the privacy and encryption technology community relies on well-earned trust, GH CCT maintains and further develops close personal ties to many smaller and larger projects in the area, giving them a chance to get to know it and learn from some of its partner projects about its services and solutions. This includes organizations such as Free Software Europe and the Open Technology Fund. CCT and GH also do outreach to high risk users and security experts. GH and CCT presents its products and solutions on their websites and in customer-facing material, and Panoramix messaging will be added to this outreach material.

Customer Relationships. GH provides secure and privacy-enhanced services for a wide variety of customers, including both corporate users and at-risk human rights activists, and maintains their relationship via providing high quality services based on open source. Similarly, CCT cultivates relationships with a large number of open source developers and projects. Both GH and CCT consider Panoramix messaging as way to increase their customers and trust by making sure the components of the messaging network are open source.

Revenue Streams. GH has a straightforward customer-based revenue stream. For normal end users, GH already charges for services such as e-mail. Therefore, GH will charge an additional fee for access to privacy-enhanced e-mail via the Panoramix messaging network. Furthermore, GH can also ensure via its running of crucial mix nodes that it can charge other e-mail providers for improved throughput. The exact pricing will be determined based on the results of user-centric testing in D7.3. The PANORAMIX ICO detailed in Section 2.3 will be also considered as alternative payment mechanism for users that engage with the privacy enhanced services that GH will offer to its customer base.

CCT has a service-oriented revenue stream. CCT charges between 5 and 30 per cent for its services in helping open source projects such as K-9 mail, based on individual needs and circumstances of the projects. While CCT is thus in a position to offer better services at comparatively lower costs than project-internal solutions or partial solutions purchased elsewhere, this service and management charge provides CCT with a steady stream of income which it can use not only to provide these services and solutions, but also to widen and improve them for existing and future partner projects. We expect CCT's specialization in mix-net messaging will provide more clients and integration opportunities for CCT, and so more revenue.

Key Activities. GH and CCT work together to provide the underlying infrastructure, both technical and social, to deploy and maintain the Panoramix mix-net messaging system developed primarily by the research partners.

Key Resources. GH has a number of servers that can serve as mix nodes in addition to its role as an e-mail provider. GH's secure infrastructure is well-suited to provide the core backbone of the Panoramix mix-networking infrastructure, and so although ultimately mix-networking messaging will be federated, GH will gain considerable first-mover advantage and maintain the

core infrastructure. CCT also, due to its experience with torservers.net, is well-equipped in helping volunteers and other organizations joining as mix nodes and messaging providers.

Key Partnerships. GH and CCT have a number of key partners. GH also works with non-profit providers such as 1984.is and Riseup that are also interested in providing mix nodes and mix-net messaging via e-mail for their existing users. CCT works with a large number of open source developers from various projects such as the Tor Project and GNUNet that are interested in contributing to the Panoramix mix-networking codebase.

Cost structure. GH's cost structure scales well with the number of users. While some of CCT's core operational costs are fixed (core staff), all project-related costs scale with adoption of our services and products (organization, accounting, auditing, etc.). Our flexible handling of this allows us to keep costs in check while providing superior services for open source projects such as PANORAMIX at very competitive rates.

5. Third-Year Exploitation and Long-Term Project Sustainability Plan

As shown earlier, each partner has a detailed exploitation plan and there is a joint exploitation plan around the engaging in a token-based ecosystem for privacy-enhancing technologies. This ecosystem will be developed jointly with other EC projects such as NEXTLEAP and independent open source developers and privacy advocates. Thus, the work of the ICO will be done by a new organization that will have a lifetime outside of any individual EC project and not dependent on the intellectual property of any of the existing partners of PANORAMIX or any other third-party. Panoramix infrastructure developed by each of the partners will therefore be one of the projects supported by this tokenized eco-system, with the tokens providing a way to incentivize the servers and software development outside of the lifetime of the project.

The goal of the new organisation, which will be a Swiss AG or Foundation, is to serve as an umbrella for privacy-enhancing technologies within Europe, with a focus on Panoramix infrastructure but a broader remit to incorporate wider use-cases. Members of the PANORAMIX project will serve on the scientific advisory board of this organization in order to align the organization with the PANORAMIX project as well as provide a way to socialize the results of the PANORAMIX project with other parts of the privacy-enhanced token ecosystem. This new organization will broadly be based on the Tor Project, but with a number of key differences, namely that it will be aimed at providing inherent financial sustainability to the larger ecosystem of privacy-enhancing technologies around Panoramix. The organisation will aim towards a clean separation between the token and blockchain ecosystem from the core mix-networking libraries that should be usable by partners and other entities (such as GRNET and SAP) without tokens, while allowing the tokenised ecosystem to support providers such as Greenhost, CCT, and non-EC providers such as *Riseup.net* who have expressed interest in supporting the mix-networking based infrastructure.

The time-line for the token-based backing of Panoramix is as follows for the third year of the project, although this time-line may change due to unforeseen regulatory developments and other legal issues:

- *January 2018*: **Found organization**: In January, found the organization ideally by working with an existing Swiss non-profit or AG.
- *February 2018*: **Finish Whitepaper**: A whitepaper will be finished, based on a more developed version of Section 2.3 and developed jointly with the NEXTLEAP project, who are also investigating encrypted messaging. This whitepaper will be circulated in order to attract attention of other projects that may be interested broadly in a token-based approach to supporting privacy-enhancing technologies or more narrowly in supporting the generic Panoramix infrastructure. The federation of initial service providers (at least two) will be chosen, who will operate with the initial organization using service contracts.
- *March-May 2018*: **FINMA ICO Submission**: With the help of a Swiss lawyer, we will submit the whitepaper for approval as a utility token. This will allow the ICO to be run

legally by Swiss law and compliant with all Swiss regulations. The Swiss jurisdiction was chosen as it is the jurisdiction with the most advanced legal procedures for tokens, and therefore it is expected that the rest of Europe will harmonize with the Swiss model.

- *June 2018*: **Initial Coin Release**: The coins will be finished and released to the public as coins on an ERC20 smart contract, where they may be purchased using Ethereum or via a KYC-compliant process by accredited investors using the appropriate contracted KYC firm such as *Bity.com*. A website will be setup explaining the ICO and the value of the privacy-enhanced tokens that will be developed by the ICO.

- *July-December 2018*: **Development of Token**: The organization will use the funding to develop the blockchain-based technology, including the actual tokens and the blockchain that keeps track of all the tokens. Furthermore, the organization will sign contract work with other organizations (including those outside the consortium) needed to consume the tokens, including both service providers and identity providers. The service providers will create a certification procedure for moving the initial federation to proof-of-stake and allow a market of identity providers to be seeded, with at least two initial identity providers chosen.

- *January 2019*: **Launch**: The software will be finished and the initial tokens produced by the ERC20 smart contract will then be capable of redeeming these coins for tokens that use a mature version of the signature schemes and Hidden-IBS approach outlined in Section 2.3. Thus, just as the PANORAMIX project draws to a close, a financially-incentivized tokenized eco-system to support the further development of mix-networking and privacy will be launched.

In parallel, the project community will be developed via a number of measures. These measures will be based on a mixture of *outreach events* that will recruit new developers and companies to the work of the consortium, as well as *developer sprints* to keep the software working and harmonized across the various project partners and stakeholders, and lastly a number of *organizational* events to keep the project internally organized around its goals. Copying the successful model of the Tor project, the goal should be that there are approximately at least biannual internal organizational events and developer sprints, ideally although not necessarily collocated.

Eventually, depending on the success of the token-based joint exploitation plan, we expect organizational events and developer after the lifetime of the project to be taken on by the new European organization developed to handle the token-based economy for privacy-enhancing technologies. Nonetheless, in Spring 2018 the new organization will not have been formed, so the organizational meeting and developer sprints will be ran directly by the PANORAMIX consortium. In Autumn 2018, the organizational meetings and developer sprints should be in process of being transferred to the new organization, so that by 2019 they can be continued after the life of the PANORAMIX consortium. It is envisioned after the life of the consortium, the new organization will continue and co-ordinate biannual organizational meetings and developer sprints.

The key organizational, outreach, and developer sprint events foreseen in the third year are given below. Note that for the third-year, outreach events by nature cannot be predicted completely, so only the major known ones will be listed here and the rest reported in the dissemination report.

- *December 2017* **Developer Sprint: Greece** In this developer sprint, organized by CCT, developers from GRNET, GH, and CCT are meeting in Athens to finish the integration needed for D7.2.

- *December 2017* **Outreach: Chaos Computer Congress (CCC) 2017** At the largest group of developers interested in privacy in the world, CCT will present the generic Panoramix open-source libraries and API.
- *January 2017* **Organizational Meeting**: A new organization will be founded, sharing members of the Advisory Board with PANORAMIX members, in January 2017, with the details discussed at the PANORAMIX Consortium meeting in Brussels on January 23rd.
- *January 2017* **Outreach: Computers, Privacy, and Data Protection (CPDP) 2017** At the largest group of potential organizational partners in Europe interested in privacy, PANORAMIX will host a panel.
- *February 2018* **Outreach - FOSDEM**: Free and Open Source Software Developers' European Meeting (FOSDEM) is the largest open source developer meeting in Europe, and a proposal to demonstrate the LEAP codebase with mix-networking has been provided.
- *Spring 2018*: **Spring Developer Sprint: TBA** In this developer sprint, the initial feedback from real users will be gathered, which will have likely led to many new bugs being discovered and work to be co-ordinated on the base open source libraries and API.
- *Summer 2018*: **Organizational Meeting**: The new organization should be finished by the time of this meeting, and will have a joint meeting with the PANORAMIX project in order to prepare future organizational independence as well as familiarize new developers partners from outside the consortium with the work done to date.
- *Fall 2018*: **Fall Developer Sprint: TBA** This developer sprint will focus on the integration of Panoramix with a token-based incentive structure for users and for running mix-networking nodes as a service, as well as in detail exploring the feedback from the actual deployment and maturing the messaging product in D7.3.
- *December 2018* **Outreach: Chaos Computer Congress (CCC) 2018** The new organization and token-based system will be submitted for presentation.
- *January 2019* **Organizational Meeting**: The new organization will have a meeting to focus on planning finances after the end of European Commission funding in January 2019, as well as a roadmap for future development.
- *January 2017* **Outreach: Computers, Privacy, and Data Protection (CPDP) 2018** The final results of PANORAMIX and future roadmap for autonomous work by the new organization after the lifetime of the EC project will be submitted for presentation, ideally as a "success story" of European support for innovative privacy-enhancing technologies.

Therefore, Panoramix and the mix-net infrastructure will not end with European Commission project funding. Like the USA-based Tor project, it will continue as an autonomous entity capable of organizing a developer community and deploying its software with both commercial and non-profit partners. Unlike Tor, Panoramix will feature a model of token-based financial sustainability that should allow the future of privacy-enhancing technologies in Europe a clear way to monetize users while supporting the maintenance of the core infrastructure, solving one of the hardest problems in the field of privacy-enhancing technologies and allowing the innovation developed in this project to continue after the lifetime of the project.

6. Conclusions

As evidenced by the above the consortium has the appropriate set of partners for tackling the ambitious goal of realizing the Panoramix infrastructure for mix-nets and bringing it to the public.

In the second year, the consortium has established initial contacts to other developers to engage them in PANORAMIX and build an own developer community. Regarding standardization, the consortium has approached the W3C and IETF, and concrete steps regarding the standardization of the Panoramix API in the IETF have been outlined.

One of the largest problems facing privacy-enhancing technologies is how to make them financially sustainable. The main US-backed privacy-enhancing technology, Tor, depends entirely on government grants and volunteers. In this deliverable, we have outlined a unique approach based on an Initial Coin Offering (ICO) and a utility token for privacy-enhancing technologies that can be utilized by PANORAMIX as part of an innovative joint exploitation plan.

Each partner also has its own individual exploitation plan. The academic partners exploit the project in several ways. By offering courses and seminars related to PANORAMIX, they reach and attract students and other researchers and get them involved with the ideas of the project, thus helping to build a community around PANORAMIX. The universities offer PANORAMIX-related topics for graduate students to write their theses on, and employ PhD students who also work on these topics. Through their combined research efforts, the universities provide theoretical background and develop state-of-the-art technologies that mix-nets are based on and hence contribute to the success of PANORAMIX. Finally, there is an opportunity to offer PANORAMIX-enhanced applications such as messaging to graduate and undergraduate students.

Individual exploitation plans for each of the industrial partners has matured and now use the Business Model Canvas. The industry partners of the project, GRNET, CCT, GH, and SAP, provide real-world use-cases that are mandated from their needs of their user-bases. This highlights the fact that the consortium has the ability to not only deliver the framework for mix-nets but also showcase it in real world scenarios affecting the bottomline experience of actual users and improving the privacy characteristics of their online experience. The exploitation plans of the industry partners presented in this deliverable are very thorough and it is expected that the Panoramix framework will be incorporated into their public and commercial offerings. The integration and exploitation of the PANORAMIX results in both academic and industrial partners have been demonstrated via Business Model Canvas for each of the use-cases, and the exploitation of the results of this project have already placed Europe on the cutting-edge of the deployment of privacy-enhancing technologies.

Finally, PANORAMIX now has a coherent third year plan to lead to success and financial sustainability outside the lifetime of the project funding. We present a new organization that can not only maintain the tokens, but also continue organizational meetings and developer sprints around the Panoramix API and codebase to maintain and grow privacy-enhancing technologies after the end of EC funding.