Benjamin Weggenmann — Ed. (SAP)
George Danezis (UCL)
Tariq Elahi (KUL)
Rafael Galvez (KUL)
Harry Halpin (GH)
Florian Kerschbaum (SAP)
Aggelos Kiayias (UEDIN/UoA)
Panos Louridas (GRNET)
Tatjana Vandenplas (MV)
Micha Zajc (UT)

Preliminary Exploitation Plan

Deliverable D2.5

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

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.1	2016-07-11	BW, FK (SAP)	Initial draft, SAP input
0.2	2016-07-29	PL (GRNET)	GRNET input, Open Source exploitation plan
0.3	2016-08-12	TV (MV)	Mobile Vikings input
0.4	2016-08-17	HH (GH)	Greenhost input
0.5	2016-08-17	BW (SAP)	Editing and review with input from all partners
0.6	2016-08-26	BW (SAP)	Updated SAP input
0.7	2016-08-29	PL (GRNET), BW (SAP)	Updated GRNET input
0.8	2016-08-30	BW (SAP)	Updated Mobile Vikings input
0.9	2016-08-30	HH (Greenhost)	Standardization, Developer Community
1.0 RC	2016-08-31	BW (SAP)	Final editing and review
1.0	2016-08-31	AK (UEDIN)	Final version and submission to the EC
1.1	2016-09-28	BW (SAP)	Revision after 1st periodic review: Added revision history, provided sections for academic partners, added remark on MV's withdrawal
1.2	2016-10-13	AK (UEDIN)	UEDIN/UoA input
1.3	2016-10-15	MZ (UT)	UT input
1.4	2016-10-17	TE (KUL)	KUL input
1.5	2016-10-17	GD (UCL)	UCL input
1.6	2016-10-21	BW (SAP)	Editing and review with input from all (industry and academic) partners
1.7	2016-10-25	RG (KUL)	Updated KUL input
1.8	2016-10-25	AK (UEDIN)	Review, minor additions and various corrections
1.9	2016-10-25	MZ (UT)	Updated UT input
2.0 RC	2016-10-29	BW (SAP)	Final editing and review
2.0	2016-10-31	AK (UEDIN)	Revised final version and submission to the EC

Executive Summary

This deliverable presents the first version of the exploitation plan for PANORAMIX. It includes our joint exploitation objectives as well as the partner-specific exploitation plans. Moreover, it describes the exploitation activities undertaken during the first year of the project. Further exploitation activities will also be reported at the end of the second year of the project (D2.6) as well as at the end of the third and final year of the project (D2.7).

The deliverable is structured in four chapters as follows:

- Chapter 1: The first chapter gives an 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 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, respectively.
- Chapter 4: This short chapter presents the conclusions of exploitation in PANORAMIX.

Contents

1. Introduction

In this deliverable the first 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 MV 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 preliminary exploitation plan is the first 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 second and third year of the project. The documents are as follows:

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

D2.6 Complete Exploitation Plan (Editor: GRNET, due: M24): We will 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 MV, 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, MV, 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 Mobile Vikings (MV). A living lab facility provided by Mobile Vikings will ensure that our system is finely tuned to the needs of the mobile users.

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.

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 projects 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 projects 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 projects commercial partners involved in the respective work-packages (GRNET, SAP, GH, MV). 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 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 Saarbrcken. We've also built bridges to other communities. Roger Dingledine, the

[1] http://mixminion.net

Director of the Tor Project, attended a WP7 meeting (Secure Messaging) involving UCL, KU Leuven, Greenhost, and Medialaan (representing MV). Discussions over mix networking and onion routing were very useful, as well as lessons from Tor in community building.

2.1.3 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 Bar-BOF 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 will attend 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.

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.

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 will incorporate 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 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, while a graduate student Kostis Kolotouros and Dr. Athanassios Angelakis are engaged at UoA. 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 organization 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. 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.

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 1026. 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. 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.

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.

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

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

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 a 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 manage to create an academic community focused on mix-net research. This goal is pursued by organizing meetings and seminars addressed to computer science students and young researchers. UT also shares PANORAMIX ideas by taking part in various workshops (like summer schools) that gather PhD students from a number of universities.

Scientific and technical goals For now (October 2016) 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.

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.

Sustainability 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.

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

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. Younger research stuff consists of: Prastudy Fauzi (Research Project Specialist), Michal Zajac (Younger Researcher), Karim Baghery, Behzad Abdolmaleki, Janno Siim (PhD students) and Annabell Kuldmaa (MSc student). 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 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.

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.

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.

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

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

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 SAPs 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 SAPs 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 techology 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.

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 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

[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

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, working with Mobile Vikings, the PANORAMIX mix-networking infrastructure will have deployment in a large-scale "Living Lab" as well as production-level deployment server-side, and possibly client-to-server side. 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.

3.4.4 Exploitation Plan of Partner MV

Addendum on departure of Mobile Vikings and new Partner: On September 13th, 2016, Mobile Vikings (MV), respectively Medialaan, expressed their intention to leave the consortium. The project steering committee approved the voluntary exit of partner MV from the consortium on September 27th, 2016. Their exploitation plan has been left here for documentary purposes.

There are currently discussions ongoing with new possible partners, including but not limited to Open Whisper Systems, the developers of K-9 Mail, and Thoughtworks. When a new partner is confirmed, they will be asked to write a new exploitation plan. This exploitation plan will be added to D7.2, which deals with the mobile messaging use-case.

Company overview VikingCo, the umbrella company of Mobile Vikings, was founded in 2009 and after 348 weeks of continuous growth has become a fully-fledged player in Belgian telecom. Right from its launch, VikingCo, an MVNO (Mobile Virtual Network Operator), disrupted the telecom market – not only with its competitive pricing for mobile data, but also with its unique focus on community and innovation. The Viking community today is 240,000 members strong.

In February 2016 Medialaan acquired VikingCo for 100%. Medialaan is the biggest Flemish commercial broadcaster in Belgium with strong TV and radio brands. With a mobile brand (JIM Mobile) already in its portfolio the acquisition of VikingCo will accelerate the new and innovative business model of Mobile Vikings while VikingCo will see its strategy reinforced by the additional opportunities Medialaan will bring along. Medialaan acknowledges the first year as a transition period where the overall mobile strategy and convergence between the companies have to be aligned.

VikingCo - Panoramix concept ideation An important goal for Mobile Vikings is to become a trusted party for the community. To understand the needs of the different stakeholders from VikingCo regarding Panoramix we investigated different use cases:

1. To protect the sources of journalists. Since Medialaan has a strong News department this use case could be relevant for the delivery of sensible and private information. VikingCo investigated this opportunity. At this moment this need is already fulfilled via *Nieuwsleaks*[10], a new platform of VTM Nieuws where users can send safe and anonymous information to our news department. The identity of the sender, location and content are not trackable. This service is integrated in the website which enables us to receive large files. The service is only relevant for big news items where strong investigative journalism is wanted. After several ideation sessions we decided to not select this use case.

[10] http://nieuws.vtm.be/nieuwsleaks

2. Corporate environment. Panoramix could be used for sensitive intercompany information between employees and important partners. However since the core business of VikingCo is community-driven, this is not the right target audience for us.

3. Enhanced secure messaging app for Vikings. A simple and secure way to enable private communication between Viking members. This use case is the most relevant of these three options since it directly impacts our members.

Exploitation strategy VikingCo wants to implement a mobile communication application on top of the LEAP service, more specifically on a WEB (/REST) API or a Black-box native client library for Android and iOS. The proposed architecture is depicted in fig. 3.1.

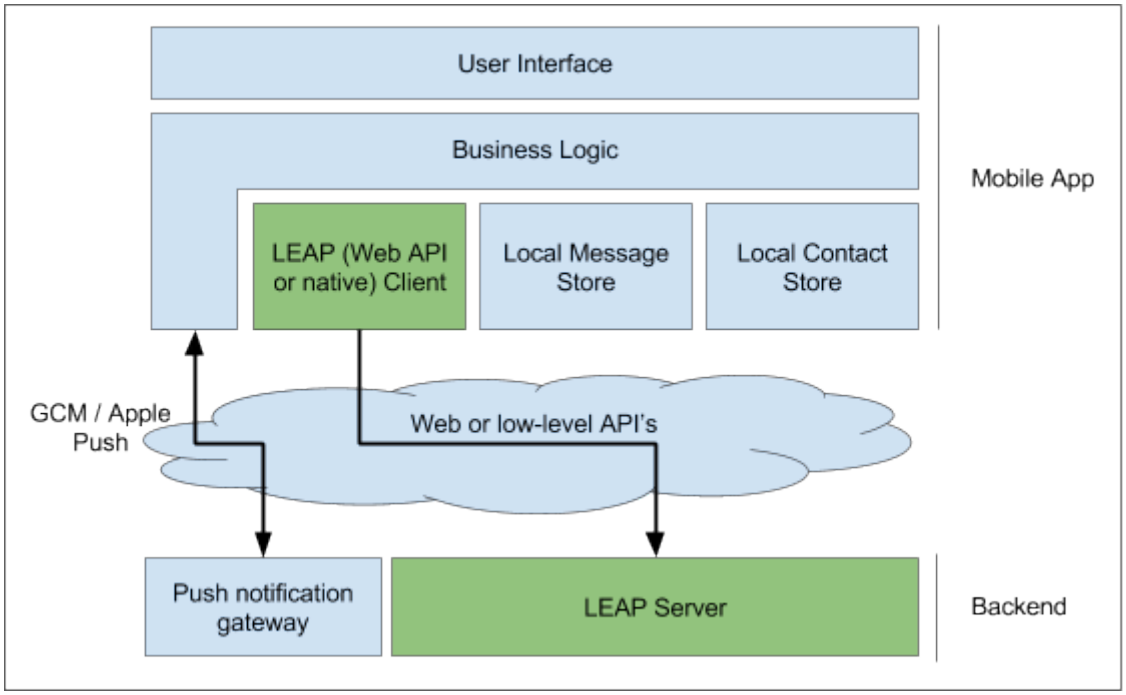

Figure 3.1: High-level architecture for proposed messenger app built on top of the LEAP service.

Deployment strategy For deploying new applications into the market, VikingCo has the facilities of the Viking Lab. The Viking Lab is a selection of (currently) 20.000 volunteers among the general Mobile Vikings population. These volunteers constitute a living lab of early adopters that are willing to test and evaluate new applications and services. VikingCo uses them to get feedback and iterate on MVPs before bringing new products to the market. As with all VikingCo products, this is the strategy we would like to take with the Panoramix project. In addition to assessing the needs of the market, the Viking Lab tests can help fine tune parameters like acceptable delay.

UI/UX exercise VikingCo wants to implement a mobile near real-time messaging application. As you can see in fig. 3.2, it resembles the UX of popular mobile chat clients like e.g. WhatsApp or Telegram.

Viability for Mobile Vikings Since several popular messaging apps like WhatsApp and Facebook Messenger are working on privacy and security, further research for the viability of a new developed messaging app has to be further investigated.

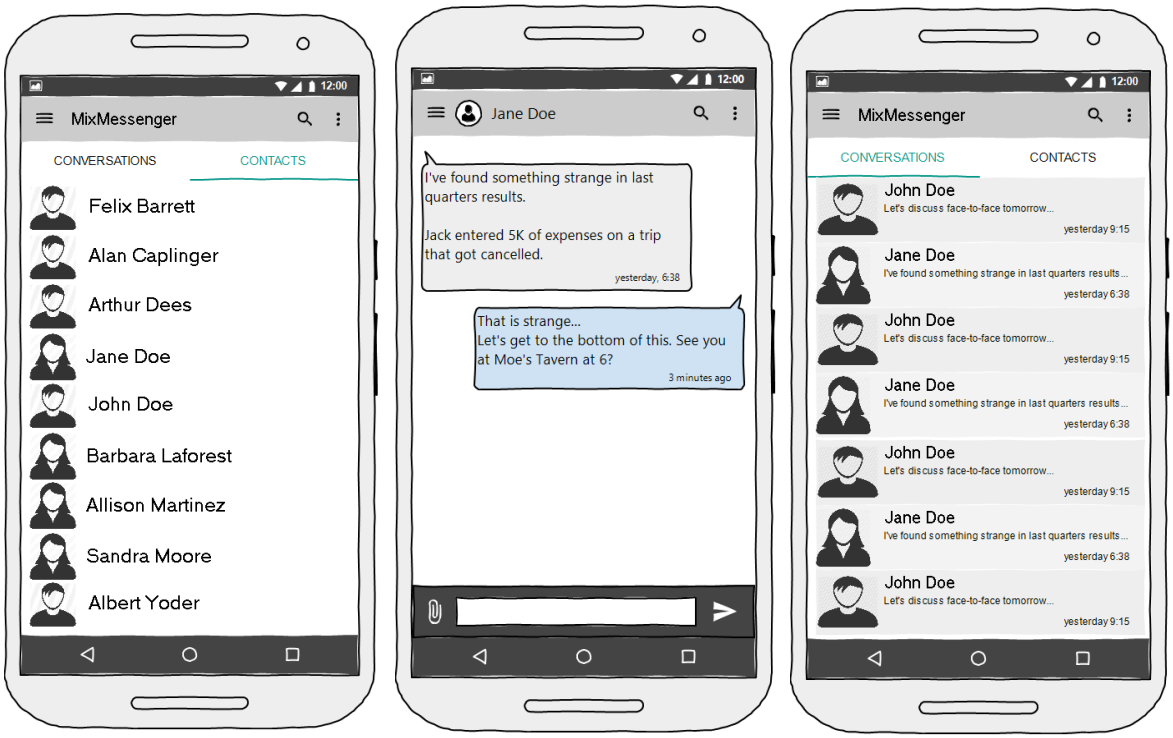

Figure 3.2: UI sketches for contact list, chat, and list of conversations.

4. 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. 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.

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.

The industry partners of the project, GRNET, MV, 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.