Tariq Elahi—Ed. (KUL)
George Danezis (UCL)
Claudia Diaz (KUL)
Benjamin Weggenmann (SAP)
Florian Kerschbaum (SAP)
Harry Halpin (GH)
Helger Lipmaa (UT)
Aggelos Kiayias (UEDIN)
Panos Louridas (GRNET)
Rafael Galvez (KUL)

Dissemination Plan

Deliverable D2.2

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	2016-02-01	TE (KUL)	Initial draft
0.1	2016-02-15	TE (KUL)	Incorporated partners' dissemination plans
1.0	2016-02-28	TE (KUL)	Final editing and review
1.0	2016-08-31	AK (UEDIN)	Final version and submission to the EC
1.1	2016-10-16	TE, RG (KUL) MW (UEDIN)	Revision after 1st periodic review
1.2	2016-10-18	RG (KUL)	Revision to incorporate updates from partners
1.3	2016-10-26	RG (KUL)	Revision to incorporate review comments
1.4	2016-10-28	RG (KUL)	Revision to incorporate second review comments
2.0	2016-10-31	AK (UEDIN)	Revised final version and submission to the EC

Executive Summary

The dissemination plan is a framework document for project activities and results. It is relevant throughout the project's lifespan, from September 2015 (M1) to August 2017 (M36) and all project partners are involved throughout. It outlines the channels through which results and key messages will be communicated to the stakeholders and audiences that have been identified to benefit from them, such as governments bodies, security practitioners, and systems designers to name a few. The execution of the plan will be measured through quantitative and qualitative measures for the sake of accountability and improvement of the project. These measures will be the basis by which assessments and updates will be carried out over the life of the project.

Contents

1. Introduction

This chapter states the purpose of the Dissemination Plan and its relationship to other project deliverables.

1.1 Purpose of document

The objective of this Dissemination Plan is to identify and organize the dissemination channels to utilize and activities to perform within the project. The aim is to promote and spread project ideals and results as well as contribute to impact creation. The document initially drafts the dissemination plan for the entire lifetime of the project, from September 2015 (M1) to August 2017 (M36). However it is expected to be reviewed and updated every year.

1.2 Relation to other project deliverables

This document is a deliverable (D2.2) for Work Package 2 - Dissemination (WP2). It is a public document which will be made available on the project website for those stakeholders interested in the dissemination plan of the PANORAMIX project. This document covers the consortium's interaction with its external audience. It provides the framework for the coordination of information flow from the project towards the outside world. Dissemination is applicable to all work packages (WPs) supporting the knowledge transfer from the consortium to the target audiences. This is especially important when considering the exploitation (Task 2.3) and standardization activities (Task 2.2). In particular, D2.2 is closely related to the following WP2 deliverables:

- Deliverable #20: D2.1-Public Web Page and Blog [UEDIN]
- Deliverable #22: D2.3-Dissemination Report I [KUL]
- Deliverable #23: D2.4-Standardization Report [GH]
- Deliverable #24: D2.5-Preliminary Exploitation Plan [SAP]
- Deliverable #25: D2.6-Complete Exploitation Plan [GRNET]
- Deliverable #26: D2.7-Report on Exploitation Activities and Updated Plan for Further Exploitation [GH, MV]
- Deliverable #27: D2.8-Scientific Advisory Board Reports [UT]
- Deliverable #28: D2.9-Dissemination Report II [KUL]
- Deliverable #29: D2.10-Dissemination Report III [KUL]

2. Dissemination strategy

A dissemination strategy comprises a number of objectives the dissemination must fulfil, the groups that will be targeted, the scope of the activities and the roles of the project partners. This chapter describes all of these components, as well as an outline of the strategy based on the Description of Action.

2.1 Objectives

The overall aim of the dissemination activities outlined in this plan is to ensure impact creation. We can break up the objectives thus:

- To continuously create awareness among the target audience about the project idea, activities, and outcomes.
- To continuously create understanding of the benefits of the project's activities and outcomes.
- To promote PANORAMIX innovations through the spread of technical results and generated knowledge within the scientific and research communities.
- To identify additional potential applications, customers and business opportunities based on the feedback to dissemination activities.

2.2 Target groups

- **Group 1: Industry.** This group comprises both business and technical experts. The communication direction can be both external to the consortium and internal towards the project partners.
- **Group 2: Security and privacy providers.** This group represents those stakeholders providing security and/or privacy solutions that want to improve their offerings by adopting novel solutions developed by PANORAMIX.
- **Group 3: Research and scientific community.** By means of knowledge and best practices transfer, PANORAMIX can have impact in scientific communities of information security, privacy, networking and distributed systems, and cryptography.
- **Group 4: Governmental bodies.** Certain governmental functions (such as e-elections) can benefit from the e-voting application thread of the PANORAMIX project.
- **Group 5: Wider public.** Informing and communicating with the public as well as fostering societal debate have already become integral constituents of the portfolio of European initiatives. Engaging in a dialogue with the public is essential to focus attention on issues of real concern such as mass surveillance and censorship. The wider public, or

ultimately the end consumer, needs to understand the exact benefits that PANORAMIX could bring in their daily life. For this audience, key-messages should focus on the overall concept rather than on specific technical solutions.

2.3 Scope of activities

We recognize that dissemination channels can have different scopes and thus differing requirements of language, format, and related delivery concerns. We distinguish between three: external, partner-internal, and project-internal. The external scope is any dissemination activity geared towards entities not associated with the project or its partners, e.g., the public. The partner-internal scope describes dissemination activities to other parts of the partner organization not involved with the project, but which could benefit from its outputs. The project-internal scope describes dissemination activities between the project partners so that they are aware of the activities and output of each other.

2.4 Outline

WP2 aims to effectively disseminate the results and innovations of the project. We will establish a holistic dissemination strategy with focus on effective communication of the project results via the public PANORAMIX website, project blog, communication of publicity materials and ensuring visibility of all dissemination events of the project. Results of the project will be published in relevant journals, prestigious scientific conferences and workshops. The project results are expected to have high impact by advancing the state of the art in mix-nets and developing a mature technology deployable in practice. This requires extensive dissemination of results to industry at technical conferences, standardization bodies, and to high-level policy-maker events. The dissemination tasks will involve all partners in parallel to the technical work in order to guarantee successful transfer of knowledge. Dissemination results will be reported in annual dissemination reports. In the privacy, computer security and cryptography community there is a longstanding tradition of providing open access to technical reports in a timely manner (mostly before conference publication) corresponding to extended versions of published papers in the main cryptographic conferences in the IACR ePrint Archive (consistent to the green standard of open access publication).

2.4.1 Task 2.1 Dissemination and Networking [Lead: UEDIN] [Contributors: all partners] (M1-M36)

Dissemination results will be reported annually in dissemination reports. The dissemination channels that will be used include but are not limited to the following: public webpage and blog of the project, project leaflets and a newsletter, publications and presentations at highly ranked and competitive conferences and scientific journals, industry fairs and exhibitions, etc. Annual dissemination reports will be delivered.

2.4.2 Task 2.2 Standardization [Lead: UEDIN] [Contributors: UoA, GRNET, GH] (M1-M36)

PANORAMIX will approach standardization in two ways. First, it will ensure that existing standards are used by the project wherever possible. This will require an investigation of de facto and de jure standards both in what regards the underlying technologies that will be developed in Work Package 3, and the use cases that are the subjects of Work Packages 5, 6, and 7. Several different project outcomes (i.e., new algorithms and protocols for mix-nets and Functional Encryption) will be relevant input for standardization efforts and international, European,

and national standardization bodies like the IEFT, ISO JTC 1/SC 27 IT Security techniques, etc. Following the above, Task 2.2 will firstly prioritize the existing standards in accordance with their relevance both for the PANORAMIX project as well as in the market/industry sector. Subsequently this task will ensure that the relevant standards are used in the project's prototypes and demonstrators. We will also contribute to standard development in areas the consortium members have the necessary expertise. We will investigate potential avenues for future standardization efforts in areas where the project makes significant advances. Finally in this task we will identify routes to ensure the uptake of the relevant standards.

2.4.3 Task 2.3 Exploitation [Lead: GH] [Contributors: all partners, SAP, Mobile Vikings, GRNET] (M1-M36)

The plan for exploitation is two-fold: First, 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. Second, the applications of the mix-net are to be demonstrated in a number of independent applications, which provide exploitation opportunities for the individual participants. Hence we will follow an open-source strategy for the development results of WP4 and the individual exploitations strategies will follow the consortium partners' business models. The feasibility of this second exploitation will already be validated in the WP5-7 use cases and demonstrators. 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.

2.4.4 Task 2.4 Advisory Board [Lead: UEDIN] [Contributors: all partners] (M1-M36)

The External Advisory Board (EAB) consists of eight members, which are experts in privacy, cryptography and security both from academia and industry. Signed Letters of Interest confirming the will to join this Board can be found in the Annex. The EAB members are expected to meet face-to-face once a year. EAB Members will be fully reimbursed for travel and accommodation expenses incurred for the attendance of the EAB Meetings and other activities of the project they attend. The EAB will provide expert advice and feedback on selected PANORAMIX deliverables. The EAB will also be consulted when the strategy for effective communication is defined. EAB meetings will be planned in conjunction with workshops or conferences of the project, where key representatives from stakeholder groups will also be invited to participate. The goal will be to present the main results of the project as well as to seek stakeholder commitment beyond the life of the project involving them in results exploitation.

2.5 Partner roles

All partners will contribute to the tasks as detailed above and specifically by participating in international conferences, promoting standardization efforts and publishing in established international journals. They will also update the news-feed blog on the public website. UEDIN (lead) will lead this WP and all its individual tasks. UoA will offer logistics support. UCL will be devoting 3 PMs to dissemination through presentation at academic and trade conference, 1 PM on standardization efforts (specification writing and reviews) and 2 PM on exploitation through deployment and releases of open-source packages. UCL will also be responsible for maintaining the bibliography of publications produced as a result of project activity on the public project website. GRNET will devote 8 PMs to standardization efforts related to e-voting standards as well as mix-nets. Another 8PMs will be devoted to general project exploitation

activities, especially relating to publicizing the mix-net software, whose development will be led by GRNET.

3. Dissemination plans

The following sections outline more concrete plans regarding the type of dissemination the different partners in the consortium will be engaging with. The different types of dissemination have been divided into General Tools (3.1) Scientific Publications and Presentations (3.2) and Industrial dissemination (3.3). The two types of partners in the consortium – Academic and Industrial – each naturally focus on different types of dissemination. Academic partners will mainly focus on publications at scientific workshops and conferences, as well as journal publications. Naturally, the industry partners will have a stronger focus on, e.g., Industry Events and Standards Proposals, but it is expected that there will be overlap between the dissemination activities of both types of partners. In the following, we highlight the main dissemination activities and how these relate to the objectives of the project and reach the respective target groups.

3.1 General Tools for Dissemination

This section describes how PANORAMIX will use social media, the website, blogging and repositories to disseminate project ideas, activities and outcomes. Blog posts and tweets will be associated with scientific publications, to increase their visibility. Similarly, code associated with publications (prototypes, etc) are advertised in the scientific papers and on social media. This cross-referencing will ensure the dissemination of PANORAMIX information will reach as wide an audience as possible.

3.1.1 Social media

An account for Twitter has been created (11/10/2016) and is now in use https://twitter.com/PANORAMIXH2020. It will be used to bring attention to project highlights and key results by tweeting published papers, linking presentations and any other PANORAMIX news. Twitter Analytics will be used to measure the effect of @PANORAMIXH2020.

Retweeting by individuals and partners in PANORAMIX is encouraged and will increase the visibility of @PANORAMIXH2020 which should result in an increased number of followers. For example, @GDanezis or https://twitter.com/Gdanezis, Dr Danezis' (UCL) twitter account is followed by 1471 other accounts including key people in the scientific and policy fields relating to privacy. To illustrate the reach, in the month of February 2016 the account reached 72.3K impressions on 10 tweets. GRNET (@grnet_gr) maintains a twitter account on which news on events and achievements are published. Thanks to its central position in the Greek research and academic community, GRNET news is widely circulated in within Greek academia.

3.1.2 Website

The PANORAMIX project has a public website (https://panoramix-project.eu/) where the consortium provides the most up-to-date details about project activity through a news feed, event calendar, and publications list.

Partner websites, either from the main page, or through a subpage or page element, link to the PANORAMIX website, thus increasing the number of potential visitors to the website. The PANORAMIX twitter feed is also visible on the website.

3.1.3 Blog

Various blog posts are used with PANORAMIX for dissemination.

- The PANORAMIX website news-feed https://panoramix-project.eu/category/news-feed/ provides a blog posting platform for project partners to advertise their individual results and activities, as well as a place for opinion pieces on relevant events. Blog posts will created based on workshops, conferences and journal articles that are produced.
- Personal blogs maintained by individual partners are used to advertise research output or to link back to PANORAMIX resources.
  - Conspicuous Chatter https://conspicuouschatter.wordpress.com/ is the personal blog of Dr George Danezis, PANORAMIX PI for UCL. The blog is used for longer, more technical, or deeper analysis relating to privacy enhancing technologies and technology public policy. In 2015 it received 22K views by 18K visitors.
- Institutional blogs maintained by the institution the project partner is employed at also provide a means of reaching a large audience.
  - UCL Information Security Blog - Bentham's Gaze https://www.benthamsgaze.org/. The Information Security Group Blog is used to advertise any scientific article to be published or presented, as well as to blog scientific opinion pieces related to their research, including PANORAMIX.
  - The KUL COSIC Cryptography Blog https://securewww.esat.kuleuven.be/cosic/?cat=11. This blog has been operating for many years and is a method used to disseminate information about projects that the COSIC group is a partner in, such as PANORAMIX. The targeted audience is the general public, and we will submit blog posts that explain the ideas and the related results of KU Leuven research in layman words.

3.1.4 Repositories

Partners' outcomes are available in repositories where both relevant software and publications are stored. Accepted publications are available as Open Access in the Academic partners' Institutional Repositories. Public documentation and code are also accessible through well known third party services.

- Institutional repositories
  - Lirias https://lirias.kuleuven.be/. Lirias is the KU Leuven institutional research repository. COSIC members submit their articles as Open Access within a 2 weeks after the notification of acceptance.
  - Edinburgh Research Explorer http://www.research.ed.ac.uk/. The Edinburgh Research Explorer is the institutional repository of University of Edinburgh staff's research outputs. Includes information on awards, projects and press coverage as well as publications, many of which are available on an Open Access basis.
  - IRIS http://iris.ucl.ac.uk/iris/. IRIS is the UCL institutional research repository. All accepted publications have to be deposited within it within 2 weeks of acceptance. Funds are available to exercise Green and Gold open access options offered by scientific publishers.

- Documentation Repository - ReadTheDocs Service https://readthedocs.org/. Documentation relating to code and prototypes will be hosted on the ReadTheDocs service. The service automatically compiles the documentation in a variety of formats including HTML and PDF every time the repository of code is updated, making it easy to publish timely and correct documentation.

- Open Access Research Repository - Arxiv http://arxiv.org/ and IACR ePrint archive https://eprint.iacr.org/. Arxiv is an open access repository for scientific works, and the eprint archive one for specialized cryptographic research. The UCL team posts articles under submission there to ensure timely dissemination, before the conclusion of the peer review process.

- Code repository GitHub http://github.com/grnet. GRNET has a long track record of producing high quality software, made available as open source and published on GitHub, under the http://github.com/grnet organization. All design and implementation software is produced using the Sphinx document preparation system and published on GRNET servers.

- Source Repository - UCL Information Security group Github Repository https://github.com/UCL-InfoSec. UCL Information Security group members disseminate open source code through the GitHub service. The service allows the wider community to interact with the code, clone and enhance the projects, and contribute back changes to improve it. The PI's GitHub profile is followed by 29 developers, and, as an example, his top repository is forked by 9 people.

3.2 Scientific Publications and Presentations

The main dissemination task that academic partners will participate in is the transfer of findings and knowledge to the third target group: "Research and scientific community". Dissemination of the research carried out at the academic partner sites[1] will be through publication and presentation at scientific conferences as well as in scientific journals. The following scientific conferences and journals will be targeted:

- Scientific Conferences - security: These are the most prestigious peer-reviewed publishing venues for technical systems research in computer security and privacy. They facilitate discussions with scientists that deliver high quality feedback, as well as collaborations on related topics.
  - IEEE Symposium on Security and Privacy http://www.ieee-security.org/TC/SP-Index.html,
  - ACM Computer and Communications Security Conference http://www.sigsac.org/ccs.html,
  - USENIX Security https://www.usenix.org/conferences/byname/108,
  - Network and Distributed Systems Security http://www.internetsociety.org/events/ndss-symposium

- Scientific Conferences - cryptography: Conferences devoted to cryptography research will allow us to receive feedback, transfer know-how and spread the awareness of the project in this specific community:

[1] University of Edinburgh (UEDIN), University of Athens (UoA), University College London (UCL), KU Leuven (KUL), and University of Tartu (UT)

  - Crypto, Eurocrypt and Asiacrypt conferences (see http://www.iacr.org/conferences/): These are the three flagship conferences of the International Association for Cryptologic Research (IACR). Every year they gather a number of cryptography theoreticians and practitioners as well as industry representatives. Due to high ranking of the conference, its proceedings are widely distributed and bring attention in the cryptographic community.
  - Real World Cryptography (RWC) (see http://www.realworldcrypto.com) is an annual conference aims to bring together cryptography researchers with developers implementing cryptography in real-world systems. The conference goal is to strengthen the dialogue between these two communities. Topics covered focus on uses of cryptography in real-world environments such as the Internet, the cloud, and embedded devices. It has grown to a main venue in the area with more than 600 participants. Consortium coordinator, Kiayias, is in the steering committee of the conference.
  - RSA Conference Cryptographers' Track (CT-RSA): CT-RSA is one of the most important cryptographic conferences. In a joint ranking for security and cryptographic conferences CT-RSA is ranked 4th (field rating) or 5th (by the number of citations)(according to Microsoft Academic Ranking, taking the last 5 years into account http://academic.research.microsoft.com/RankList?entitytype=3&topdomainid=2&subdomainid=2&last=5&orderby=6). Similar to Asiacrypt, it gathers both academic and industry community experts focused on cryptography and security. CT-RSA conference receives a lot of attention from both the academic and industry communities.
  - Africacrypt conference: During the Africacrypt conference we will target the academic community focused on various aspects of computer security and cryptography. The articles will appear in Springer's Lecture Notes on Computer Science as well as at the IACR web-archive eprint.

- IEEE European S&P Symposium (EURO S&P). Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. Following this story of success, IEEE initiated the European Symposium on Security and Privacy (EuroS&P), which is organized every year in an European city.

- ESORICS (http://homepages.laas.fr/esorics/) is focused on computer security in general. It establishes a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas. Accepted articles are published in Springer's Lecture Notes on Computer Science.

- *ACM Workshop on Privacy in the Electronic Society* is a highly reputed workshop where researchers present novel works on all theoretical and practical aspects of electronic privacy, as well as experimental studies of fielded systems. The articles are included in the ACM Digital Library.

- The Summer Research Institute workshop: The Summer Research Institute is an annual event hosted by the École Polytechnique Fédérale de Lausanne (EPFL). It gathers together young researchers like computer science students and PhD students. During the workshop we would like to achieve two goals: make the audience aware of the PANORAMIX goals and make it understand benefits and opportunities that come with the project. This channel works closely with channels mentioned above, i.e., with conference papers and presentations of recent developments in the project.

- Crypto.Sec Day http://crypto.di.uoa.gr/CRYPTO.SEC/Crypto.Sec.Day.html is an annual event hosted by the University of Athens. It gathers young research community like computer science students (both graduates and undergraduates) and PhD students. During the workshop we would like to achieve two goals: make audience aware of the PANORAMIX goals and make it understand benefits and opportunities that come with the project. This channel works closely with channels mentioned above, i.e. with conference papers and presentations of recent developments in the project.

- The following journals are the top specialized journals for research in technical privacy enhancing technologies and cryptography. They allow us to widen our audience both in the cryptography and the privacy communities.

  – IEEE Transactions on Information Forensics & Security
  http://signalprocessingsociety.org/publications-resources/ieee-transactions-information-forensics-and-security,

  – Theoretical Computer Science
  http://www.journals.elsevier.com/theoretical-computer-science/,

  – Journal of Cryptology
  https://www.iacr.org/jofc/,

  – IEEE Transactions on Information Theory
  http://www.comm.utoronto.ca/trans-it/,

  – Designs, Codes and Cryptography
  http://link.springer.com/journal/10623,

  – PoPETs
  https://petsymposium.org is an open access journal associated with the Privacy Enhancing Technologies Symposium, a crucial meeting point for privacy researchers.

3.3 Industrial dissemination

The industrial partners in PANORAMIX –GreenHost, SAP and Greek Research and Technology Network (GRNET)– are geared more towards policy and standardization in their dissemination. Below are descriptions of how engagement with industry standards bodies will be achieved. The list of Industry Events illustrates the various platforms where PANORAMIX partners will have the opportunity to engage with all of the target groups identified in Section 2.2.

3.3.1 Standards Proposal

- Messaging Malware Mobile Anti-Abuse Working Group conference https://www.m3aawg.org/. Our objective would be to discuss the impact of mix-networking on spam prevention with industry standards body.

- Internet Engineering Task Force Meetings (IETF) https://www.ietf.org. Discuss future network-level standards with the world's leading standards body for global internet protocols. Meets quarterly.

- World Wide Web Consortium (W3C) meetings https://www.m3aawg.org/. Discuss impact of mix-networking on application-level security and privacy. Meets bi-annually.

3.3.2 Industry Events

These events can be used to inform the general public and industry community about the PANORAMIX project and its goals. Presence of industry representatives makes it also an

opportunity for further exploitation. The goal is to spur the discussion with them on, as well as to get feedback in order to review and improve our work and possibly spark new ideas.

Furthermore, we aim at bringing the need for data protection and our work on privacy-preserving techniques to the attention of existing customers and business partners, which in turn support us in raising awareness among product owners about our work on privacy-preserving technologies (such as mix-nets and differential privacy).

- United Nations Internet Governance Forum http://intgovforum.org/cms/. Discuss importance of metadata protection and PANORAMIX results with industry and government representatives.

- RSA conference http://www.rsaconference.com/. Demonstrate latest prototype of privacy-preserving secure messaging at world's largest industry conference on security.

- CCC http://www.ccc.de/en/. Chaos Communication Congress https://en.wikipedia.org/wiki/Chaos_Communication_Congress. Present and discuss PANORAMIX results at Europe's larger gathering of privacy advocates and coders.

- HOPE http://hope.net/. Present and discuss PANORAMIX result at USA's gathering of security privacy advocates.

- DEFCON https://defcon.org/. Present and discuss PANORAMIX result at world's larger gathering of security specialists, privacy advocates and coders.

- Internet Freedom Festival https://internetfreedomfestival.org/. Demonstrate latest prototype of privacy-preserving secure messaging at Europe's anti-circumvention gathering for human rights defenders. This event provides a venue to interact with users, practitioners, and advocates about topic related to privacy on the Internet. It has become a meeting point for researchers, software developers and the general public where we will exchange ideas, foster collaborations with other possible industry partners, and identify unsolved problems that real users need to face.

- Cryptorave https://cryptorave.org/. Demonstrate latest prototype of privacy-preserving secure messaging at Brazil's largest gathering of privacy advocates.

- RightsCon https://www.rightscon.org/. Discuss importance of metadata protection and PANORAMIX results for with secure providers and human rights defenders.

- International World Wide Web Conference http://www.iw3c2.org/ is a premier forum for discussion and debate about the evolution of the Web, the standardization of its associated technologies (like PANORAMIX), and the impact of those technologies on society and culture.

- Black Hat Briefings https://www.blackhat.com/ Present and discuss PANORAMIX results with the brightest professionals and researchers in the industry. Black Hat is the most technical and relevant global information security event series in the world.

- Workshop—Tor developers meeting. This event brings together key players from the Tor development community, and provides an excellent venue to disseminate results and ideas from the PANORAMIX project.

- E-enabled elections in Estonia: Forum on research and development workshop 2015: E-enabled elections in Estonia is an event that gathers industry and academic experts and researchers whose work is relevant to the Estonian e-voting system. government representatives also participate in the audience.

3.3.3 Media

Magazines provide an ideal channel to disseminate privacy problems and PANORAMIX solutions to other fellow scientists and engineers. They will understand the positive qualities of mix-networks through less rigorous presentations aimed at enhancing the understanding.

- ACM Transactions on the Web http://tweb.acm.org/, IEEE Internet Computing http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=4236.
- BBC, The Register, Press review: http://sec.cs.ucl.ac.uk/ace_csr/news_announcements/. The UCL Information Security group has a well establish relationship with key technical correspondents in the UK press. We plan on using those contacts to disseminate results.

3.3.4 Enterprise Internal Events

Internal Events in companies are an ideal channel raise the awareness of PANORAMIX outcomes among development units which would benefit from the ease of use and clear descriptions of the properties that PANORAMIX offers.

- SAP Security Summit. Talk and discussion about possible areas of application and benefits of our work and research. SAP-internal events provide a great platform to reach stakeholders from other SAP development units, who are the main target for SAP's exploitation activities.
- SAP d-kom. Talk, interactive workshop, or demonstration to promote results to colleagues and other departments within SAP.

4. Progress monitoring

To monitor the progress of the dissemination activities, each of them will be summarised in a record. To evaluate this progress, we identify indicators along with their corresponding yearly targets.

4.1 Record format

Each partner will keep track of their efforts in dissemination activities in order to provide a means for accountability and improvement. To facilitate this a common template record has been created and is stored on the project website for use by all of the consortium's members.

Table 4.1 describes the record format for academic dissemination activities, such as scientific conferences, workshops and presentations.

Title of venue	
Location	
Date	
Type	Conference, workshop, presentation
Partners involved	
People involved	State if PI, postdoc, student, with name
Relevance to the project	
Resources spent	

Table 4.1: Record format for an academic dissemination activity

Table 4.2 describes the record format for industrial dissemination activities.

Activity	
Location	
Date	
Type	Presentation, training, product innovation, tech transfer
Partners involved	
People involved	State if PI, postdoc, student, with name
Relevance to the project	
Resources spent	

Table 4.2: Record format for an industrial dissemination activity

4.2 Performance indicators

The key performance indicators and yearly targets (in Table 4.3) have been identified across all partners of the project. Each of the target groups described in section 2.2 will engage in

a reasonable number of dissemination activities that will ensure that PANORAMIX awareness and impact keep growing over time.

Dissemination Type	Examples	Target (per year)
User-facing website articles and blog posts	ZDNet, Register, CNet, Ars Technica, blogs, social media	12
Research Conference	ACM CCS, Crypto, Eurocrypt, PETS, ESORICS, Asiacrypt, TCC, PKC, Financial Cryptography, IEEE Security and Privacy, and others.	6
Research Journal	International Journal of Applied Cryptography, IEEE Transactions, Journal of Computer Security, and others.	3
Policy Conference	Digital Enlightenment Forum, CPDP, European Parliament, national-level meetings	3
Industry Event	LeWeb, RSA, Trust in the Digital World, CCC, IETF, W3C, TPAC	6
Media Event	Wired (Threat Level), national news papers like The Guardian	2
Training Courses, Videos and Documentation	MOOCs, Youtube video, training, lecture series	3

Table 4.3: Dissemination Key Performance Indicators

5. Conclusion

This document presents the general outline for the dissemination strategy for the PANORAMIX project. This version of the plan has been created to bootstrap the dissemination process and get all partners aligned in a common framework. It is expected that as the project progresses all the partners will participate in dissemination activities targeting different audiences; PANORAMIX as a project will benefit as a whole through the overall action of all of them, leveraging the expertise of individual partners in certain venues.