Ref. Ares(2019)559601 - 31/01/2019

Michal Zajac—Ed. (UT)
Mirjam Wester (UEDIN)
Aggelos Kiayias (UEDIN)

Scientific Advisory Board Reports

Deliverable D2.8

January 31, 2019
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Dissemination Level: Public

Revision History

Revision	Date	Author(s)	Description
0.1	03/11/2018	MW (UEDIN), MZ (UT)	All notes from the meetings collected and put together.
0.2	27/11/2018	MZ (UT)	Added Sven Heiberg report.
0.3	10/12/2018	PC (UoA)	Review and proofreading.
0.4	13/12/2018	AK (UEDIN)	Editorial pass.
0.5	20/12/2018	MZ (UT)	Restructuring, after WPLB discussion.
0.6	22/12/2018	MW (UEDIN)	Further revision.
1.0	31/01/2019	MW(UEDIN)	Final version submitted to EC.

Executive Summary

This deliverable gives an overview of the involvement of the external advisory board (EAB) in the PANORAMIX project. The document was created mainly based on PANORAMIX members' notes of discussions during meetings with the EAB as well as some written feedback. Section 3 consists of an overall report of the project provided by Sven Heiberg from the Smartmatic-Cybernetica Center for excellence in Internet Voting.

Contents

1. EAB members

List of the members of the PANORAMIX advisory board, their affiliation and expertise relevant to supporting PANORAMIX.

- **Jacques Bus**

  Affiliation Former Head of Unit, Trust and Security. Digital Enlightenment Forum/Digitrust.

  Expertise Policy support and networking with existing EC projects.

- **Marit Hansen**

  Affiliation Unabhaängige Landeszentrum fur Datenschutz

  Expertise Deputy Privacy & Information Commissioner of Land Schleswig-Holstein, Germany, and Deputy Chief of Unabhaengiges Landeszentrum fuer Datenschutz (ULD). Within ULD Marit Hansen is in charge of the 'Privacy Enhancing Technologies (PET)' Division and the 'Innovation Centre Privacy & Security'.

- **Gus Hosein**

  Affiliation Privacy International

  Expertise Director of Privacy International, researcher in Privacy Enhancing technologies and Surveillance Studies.

- **Sven Heiberg**

  Affiliation Smartmatic–Cybernetica Center for Excellence for Internet Voting.

  Expertise Since 2005, Estonia has employed nation-wide Internet voting, up to now being the only country to do so. Sven Heiberg has been the i-voting project leader at the vendor since then. He currently serves as a member of the Estonian Internet Voting Committee. Sven is looking for ways to provide usable, secure and transparent Internet voting in Estonia and abroad.

- **Bart Preneel**

  Affiliation KU Leuven.

  Expertise Professor at COSIC group, former president of the International Association for Cryptologic Research, project manager of the ECRYPT II network.

- **Omer Tene**

  Affiliation International Association of Privacy Professionals / College of Management School of Law, Rishon Le Zion.

  Expertise Vice President of Research and Education at the International Association of Privacy Professionals. Managing Director of Tene & Associates and Deputy Dean of the College of Management School of Law, Rishon Le Zion, Israel (on a leave of absence). Affiliate Scholar at the Stanford Center for Internet and Society; and a Senior Fellow at the Future of Privacy Forum.

2. EAB meetings

In terms of what was originally envisioned to be in this deliverable, the description in the Panoramix DoW states: *After each EAB meeting EAB will write a report with observations, recommendations and conclusions on actions for increasing the project impact. A summary of all reports will be compiled at the end of the project.*

In practice, we deviated slightly from this description. Instead of taking up valuable time from the members of the EAB by requiring them to compile reports, we asked for their observations and recommendations by means of discussions between the advisory board and the PANORAMIX team. This section describes the meetings, the EAB members present and summaries of the discussions and feedback to the project.

2.1 Saarbrücken meeting 03/21/2016

2.1.1 External Advisory Board members in attendance

- Jacques Bus **JB (EAB)**
- Sven Heiberg **SH (EAB)**

2.1.2 PANORAMIX members in attendance

• Aggelos Kiayias **AK** (UEDIN) • Athanasios Angelakis **AA** (UoA) • Helger Lipmaa **HL** (Tartu) • Michal Zajac **MZ** (Tartu) • Panos Louridas **PL** (GRNET) • George Tsoukalas **GT** (GRNET) • Tariq Elahi **TE** (KUL) • Rafael Galvez **RG** (KUL) • Anna Piotrowska **AP** (UCL) • Sacha van Geffen **SvG** (GH) • Meskio **Me** (GH) • Florian Kerschbaum **FK** (SAP) • Benjamin Weggenmann **BW** (SAP) • Raf Degens **RD** (MV) • Varac **Va** (GH)

2.1.3 Meeting agenda

1. Status of the project (WP1-WP2) **AK**
2. WP3, Mix-net and Privacy Research: Overview **AP**
3. Mix-net and Privacy Research: Privacy-preserving Statistics **FK**
4. Mix-net and Privacy Research: Vuvuzela Report **AK**
5. Mix-net and Privacy Research. Zero-Knowledge Proofs **HL**
6. Mix-net and Privacy research: cMIX report **AA**
7. WP4 Status: Mix-net Implementation **GT**
8. Discussion. Advisory board recommendations moderator **AK**
9. Use-case (WP5) : E-voting. Objectives and Roadmap **GT**

10. Use-case (WP6) : Statistics. Emphasis on Differential Privacy and Text Anonymization **BW**
11. Use-case (WP7) : Messaging. Objectives and Roadmap **HH**
12. Use-case (WP7) : LEAP Demo **Me Va**
13. Mix-net and Privacy Research (WP3) **TE**
14. Use-Case (WP7) : Update on Partner Mobile Vikings **RD**
15. Privacy and Ethics **JW**
16. Discussion. Advisory board recommendations, moderator **AK**

2.1.4 EAB observations

SH (EAB) There are some things with the API that I would like to point out.

- *Who is the user of this API?* There are many stakeholders that could be interested in the API and they have slightly different needs. If I were to enumerate, then we have Election Organizers, Election IT team, E-voting software developers, Mix-service providers, Voters and Observers/Auditors.
- *How do they relate to the API?* Is this a product that I can purchase/take and implement in the election, is this framework, so that different implementers/service providers can be compatible?
- *What are the use-cases or scenarios of this API?* From i-voting perspective I really see two – using mixnet simply for shuffle and using it as a decryption mixnet. Let's take the example of decryption mixnet – we are really solving 2 problems here – that of a private key protection (usually done by HSMs) and verifiable tally, maintaining voter privacy. Which aforementioned users would have to interact with the API in what manner to have MofN threshold scheme for decryption mixnet and occasional shuffle before the actual decryption?
- As an election organizer I need to understand how this can be deployed – who is responsible for hosting what – also how can I select the suitable cryptosystem/bitlength (even if its just a label) and threshold. IT wants to understand how to run the whole thing during the election and then there are Auditors who should verify that the mixnodes are performing correctly and this auditors might need access to different levels of proofs:
  1. trusting the mixnet for verification
  2. trusting some external implementation for verification
  3. trusting its own implementation for verification
- When the mixnet with threshold decryption requires the nodes exist longer in time – they need to participate in election key generation, then the shuffle nodes we can really add on the fly if this were somehow to be shown to add value to the specific setup - here the compliance with the API could be a prerequisite that the election owner could state for the interested audience.
- *What kind of interface does the API provide?* This question is multifold – what kind of transport mechanisms (such as HTTP, USB) the API supports AND how is the data encoded. Moreover, how is the data encoded in such a manner that some generality in terms of algorithms and bitlengths can be assumed. I am not aware of any unified approach in the field of mixnets. If I look towards e.g. X509 where similar problems have been solved, I see ASN.1 as the notation that is used.

2.1.5 EAB recommendations

SH (EAB) What is really necessary is to show who is the user of the API, what are her use-cases/scenarios and how these scenarios are implemented using the API.

2.1.6 EAB conclusions on actions

SH (EAB) Pick-out 1-2 scenarios from all 3 application fields and see if we can converge to a unified API and have an illustrated example for each of these scenarios, even if its just bunch of UML sequence diagrams. From the voting perspective the API seems to be quite straightforward: Setup, Prepare, Receive, Verify proof, Process, Send, Send proof.

2.2 Brussels meeting 01/24/2017

This meeting in Brussels was prior to the first of three PANORAMIX dissemination activities at CPDP.

2.2.1 External Advisory Board members in attendance

- Bart Preneel **BP (EAB)**
- Gus Hosein **GH (EAB)**
- Jacques Bus **JB (EAB)**
- Marit Hansen **MH (EAB)**
- Omer Tene **OT (EAB)**
- Sven Heiberg **SH (EAB)**

2.2.2 PANORAMIX members in attendance

• Moritz Bartl **MB** (CCT) • Harry Halpin **HH** (Greenhost) • Dimitris Mitropoulos **DM** (GRNET) • George Korfiatis **GK** (GRNET) • Giorgos Tsoukalas **GT** (GRNET) • Panos Lourdes (GRNET) **PL** • Claudia Diaz (KUL) **CD** • Rafael Galvez **RG** (KUL) • Tariq Elahi **TE** (KUL) • Kali Kaneko **KK** (LEAP) • Benjamin Weggenman **BW** (SAP) • Ania Piotrowska **AP** (UCL) • George Danezis **GD** (UCL) • Aggelos Kiayias **AK** (UEDIN) **AK** • Mirjam Wester **MW** (UEDIN) • Thomas Zacharias **TZ** (UEDIN) • Pyrros Chaidos **PC** (UoA) • Helger Lipmaa **HL** (UT) • Michal Zajac **MZ** (UT) • Annabell Kuldmaa **AK** (UT) • Mooness **Mo** (LEAP)

2.2.3 Meeting agenda

1. Status of PANORAMIX (WP1 & 2) **AK**
2. Mix-net and Privacy Research Overview (WP3) (UCL)
3. WP3 **HL MZ**
4. WP3 **CD TE RG**
5. WP3 **AK TZ PC**
6. WP4 Overview (KUL, GRNET)
7. Mix-net Demo and video. (GRNET)

8. WP5 Overview (GRNET, UEDIN)
9. WP5 Demo (GRNET)
10. Discussion & Comments on Demo, Video etc.
11. Discussion and Advisory Board Recommendations for Morning Session.
12. WP6 **BW**
13. WP6 Demo
14. WP3 Next steps (UCL)
15. WP7 (GREENHOST)
16. Demo for WP7
17. K-9 Presentation **MB**
18. Discussion & Advisory board recommendations for Afternoon session
19. Advisory board meeting with WPLB

2.2.4 EAB observations

This section lists the main observations that were made by the EAB during the discussion at the end of the January 2017 meeting, followed by PANORAMIX's clarifications at that time.

JB (EAB) Regarding the e-voting, how do you see the e-voting platform? At home, or on a certain computer?

PL The e-voting system Zeus – already exists and PANORAMIX will serve as back-end to Zeus. The challenge is how to bring others to code their own mix-nets. Regarding where people vote, there are a number of things to take into consideration. First of all, it should not be possible to connect a vote to a person. The vote must be discrete and secure. Furthermore, it is very important that a voter can not be coerced into a vote. One of the solutions to ensure no coercion is to include the option for each individual to vote as many times as they like. You can always come again later to vote.

JB (EAB) Great showcase but not ready for general elections. Culture and types of attacks different in different countries. There are many different threat models.

PL Zeus came about because of new voting laws. Zeus has been already proved useful in voting for university governing body – ballot boxes were stolen and Zeus allowed for the elections to take place. Of course, e-voting is a more complicated problem than that PANORAMIX will solve, but it is already being used in a variety of elections.

MH (EAB) People will want help/guidance to understand what they have to do. Thus, there are legal responsibilities attached. What is the real solution? How do people get the information? Be enlightened? Where do they get their answers?

CD One needs to keep in mind that PANORAMIX won't be a single application, it will be a package of software. The goal is that it will be very easy to set-up separate mix-networks. The objective for the PANORAMIX project is to build the software.

TE As the project futher develops, people will be informed through our dissemination efforts. In addition to that, we will be providing documentation. One of the things we are considering is to invite people to open workshops Developers will be invited to use the platform.

BP (EAB) Great research. Is secure messaging possibly easier? E-mail is an unsolved problem.

HH E-mail makes more sense (than secure messaging). Anything better is a win. WhatsApp/Wire/Signal – all of them are a little bit different.

SH (EAB) I am looking at this through the eyes of a vendor. Estonia has been doing internet voting for 10 years. Mix-net was there is 2003, only now have we reached that. In the next election, we hope to use verifiable shuffling for data to give to 3rd party auditors. One wishes PANORAMIX was earlier then it could have been piloted. There are already some solutions. In that respect, it may be a bar for PANORAMIX to jump over. How will the software integrate?

GH (EAB) Impressed by your work, the use-cases. We need this, it will help this sector push for policy change. Companies are lacking in privacy.

MH (EAB) Data Protection Authorities are interested in state-of-the-art. If you have this, the enforcement authorities will be your friend.

2.2.5 EAB recommendations

The recommendations put forward by the members of the EAB in attendance at the meeting in January 2017, were the following:

JB (EAB) suggested it would be very valuable to connect to normal users, and to work at creating a community. One of the ways this could be achieved would be to look at which actions are around and engage with those. In addition to that, it might be interesting to engage with social experts. Another avenue to consider is the trust of big clients. He put forward that it may be interesting to work with hacking to demonstrate that it is non-breakable. As a suggestion, a final workshop or hackathon open challenge could be considered – if you manage to break it you win.

GH (EAB) gave the advice to be preparing where you want to be in 10 years. He also added to JB's point of doing more engagement and recommended reaching out to NGOs, electoral commissions, institutions, etc.

MH (EAB) raised the point that is was important to make it clear how PANORAMIX relates to GDPR. Looking at the problem from only a scientific point of view is not so interesting. She stressed PANORAMIX should see what is necessary to fulfil the needs of others – people from other disciplines.

BP (EAB) Added to the other EAB members by stating he had just one piece of advice – get buy-in.

2.2.6 EAB conclusions on actions

GH (EAB) Don't wait with dissemination till the end of the project.

2.3 Advisory Board Meeting – Tele Conference 10/27/2017

This was a call set up to specifically get the advisory board's point of view on a number of critical issues within the PANORAMIX project. It was a very frank discussion.

2.3.1 External Advisory Board members in attendance

- Jacques Bus **JB (EAB)**
- Bart Preneel **BP (EAB)**
- Gus Husein **GH (EAB)**
- Sven Heiberg **SH (EAB)**

2.3.2 PANORAMIX members in attendance

• Aggelos Kiayias **AK** – Overview • George Danezis **GD** – WP3 • Panos Louridas **PL** – WP4 • Ben Weggenman **BW** – WP6 • Claudia Diaz **CD** – WP7 • Harry Halpin **HH** – WP7 • Moritz Bartl **MB** – WP7 • Mirjam Wester **MW** – note taking

2.3.3 Meeting agenda

1. PANORAMIX progress overview **AK**
2. PANORAMIX research overview **GD**
3. Discussion with EAB

2.3.4 EAB observations

AK EAB, are there any things we need to be careful/mindful of? Could you give advice from projects you have been involved with?

GH (EAB) That is the most difficult question ever. I'm impressed with the plans you have so far. However, can't advise without knowing more. Would be happy to have a one-on-one conversation with WP leader(s) to further discuss concrete plans. The law doesn't prohibit PANORAMIX nor does it enable it. Happy to help you place it in a broader perspective.

2.3.5 EAB recommendations

AK Research in PANORAMIX going very well, but still some deliverables are rejected, no word about the research. How do we prevent this at the end of the project?

JB (EAB) The PO plays an important role.Talk to the PO.

BP (EAB) Pro-actively change the things that reviewers have asked for previously. Object if it is outside of contract.

AK We are heavy on the technical side, lightweight on the legal side. What about the legal ramifications of PANORAMIX?

JB (EAB) I would like to see an event with participants from usability and law etc. to discuss these matters. However, you shouldn't spend too much time on this for a deliverable.
GH (EAB) What is needed is a softer social edge to the project. Don't frame it "Since Snowden...", talk about social goals that you are trying to achieve.

2.3.6 EAB conclusions on actions

JB (EAB) Talk to the PO.

2.4 Brussels meeting 01/23/2018

The second meeting in Brussels, again prior to CPDP - in this case the project had a panel to disseminate the project.

2.4.1 External Advisory Board members in attendance

- Gus Hosein **GH (EAB)**
- Marit Hansen **MH (EAB)**

2.4.2 PANORAMIX members in attendance

• Vasilios Mavroudis **VM** • Aggelos Kiayias **AK** • Benjamin Weggenman **BW** • Claudia Diaz **CD** • George Danezis **GD** • Harry Halpin **HH** • Michal Zajac **MZ** • Mirjam Wester **MW** • Moritz Bartl **MB** • Panos Louridas **PL** • Pyrros Chaidos **PC** • Rafael Galvez **RG** • Rebekah Overdorf **RO** • Sacha van Geffen **SvG** • Thomas Zacharias **TZ**

2.4.3 Meeting agenda

1. PANORAMIX: use-case implementations
   WP5 - GRNET **PL**
   WP6 - SAP **BW**
   WP7 - CCT/GH **MB**
2. PANORAMIX:
   WP4 / WP7 integration
   WP4
   D4.3 & D7.2
3. EAB meeting
   Project Status
   Project - Final Year
   Integration platform
   Project Legacy

ICO

Outreach/community engagement

Discussion & Recommendations

4. Wider Community

PANORAMIX overview

Research presentations

Use-case presentations

2.4.4 EAB observations

Overall EAB felt the project was very much on track and were looking forward to the CPDP panel.

2.4.5 EAB recommendations

On this occasion the EAB didn't have many points of feedback.

2.4.6 EAB conclusions on actions

On this occasion the EAB didn't have many points of feedback.

2.5 Athens meeting 24-25/09/2018

The September 2018 meeting in Athens was our penultimate project meeting, specific feedback was elicited from our EAB on how to incorporate their feedback on the PANORAMIX project in the current Deliverable.

2.5.1 External Advisory Board members in attendance

- Bart Preneel **BP (EAB)**
- Sven Heiberg **SH (EAB)**

2.5.2 PANORAMIX members in attendance

• Aggelos Kiayias **AK** • Benjamin Weggenman **BW** • Claudia Diaz **CD** • Dimitris Mitropoulos **DM** • Giorgos Tsoukalas **GT** • Harry Halpin **HH** • Michal Zajac **MZ** • Mirjam Wester **MW** • Moritz Bartl **MB** • Panos Louridas **PL** • Pyrros Chaidos **PC** • Rafael Galvez **RG** • Sacha van Geffen **SvG** • Thomas Zacharias **TZ**

2.5.3 Meeting agenda

1. Introduction - Project Status **AK**
2. Infrastructure **RG**
3. e-Voting **DM**
4. Privacy preserving statistics **BW**
5. Messaging **CD** **MB**
6. WP4/WP7 integration

7. Use-case Deliverable Discussion. D4.4, D5.4,D6.2, D7.3
8. Legal Perspective - GDPR **MK**
9. Standardisation **HH**
10. Project Legacy: ICO **HH**
11. Outreach/community engagement **MB**
12. Deliverable discussion D1.5, D2.7, D2.8, 2.10
13. Advisory Board Discussion & Recommendations

2.5.4 EAB observations

SH (EAB) I will provide PANORAMIXwith his notes from the meeting in Saarbrucken. Way back then I proposed the use of Verificatum, and look it has been implemented. I will provide written feedback on the project.
BP (EAB) The PANORAMIX project is going extremely well because of the ecosystem. PANORAMIX is a very strong academic project. Sewing in backdoor to make users accountable – this is a matter of principle that's why we won't do that.

2.5.5 EAB recommendations

BP (EAB) You should try to standardise (go to ETSI).

2.5.6 EAB conclusions on actions

BP (EAB) Prepare a report and send to the advisory board for approval. Ask EAB for support on things that may cause problems with the reviewers (act proactively).
SH (EAB) Denote who attended each meeting.

3. Final conclusion

The report below was provided by Sven Heiberg after attending the PANORAMIX project meeting in Athens in September 2018.

The 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.

One of those high-value applications that was aimed by the project is online voting. In case of online voting we have contradictory requirements – ballot secrecy from the one end and verifiable integrity of the tally from the other end. Remove one of those requirements and it is straightforward to provide a solution, for online voting to be usable in actual elections, both properties have to be provided.

A family of online voting protocols rely on the mix-nets for privacy preserving verifiablity of the tally, these include Helios, Zeus, Estonian IVXV and Norwegian eValg (discontinued) system. Already in 2015 we had industrial-grade efficient open-source implementations of verifiable re-encryption mix-nets in the random oracle model. PANORAMIX project has focused on the CRS model and has proposed shuffle arguments that are efficient enough to attract the attention of practioners. There also exist example implementations of these arguments. Yes, the arguments in random oracle model remain more efficient, but as of 2018 there is a choice to go with the CRS model and abstain from the random oracle model. This option is important as the random oracle is a theoretic construct that does not exist in practice and the heuristics we rely on as a substitution cannot be proven secure. Before the PANORAMIX project no such choice existed. There is body of additional reasearch done within the PANORAMIX project - on bulletin boards, block-chain - that is of importance to the field of secure online voting.

The PANORAMIX project gathered under the same umbrella very different applications - e-voting, privacy of email communication, privacy preserving information gathering from IOT devices. The PANORAMIX framework provides generalised approach to set up mix-net instances for the needs of particular application, whereas use-case teams work on more specific details. From the project meetings one leaves with a feeling that albeit variety of organizations are involved, this is a single team working on the same goal. For me it is particularly interesting to see the plans to further the sustainability of the PANORAMIX beyond the project lifetime.