FENTEC

D2.14 Project Advisory Board Workshop Report Y2

Document Identification			
Status	FINAL	**Due Date**	31/12/2019
Version	1.0	**Submission Date**	20/12/2019

Related WP	WP2	**Document Reference**	D2.14
Related Deliverable(s)	D2.1	**Dissemination Level (*)**	PU
Lead Participant	ENS	**Lead Author**	Michel Abdalla
Contributors	ATOS, ENS, FUAS, KU Leuven, KUD, UH, WALLIX, XLAB, PAB Members	**Reviewers**	Marco Lewandowsky (FUAS) Hendrik Waldner (UEDIN)

Keywords:
Project Advisory Board, meeting, minutes, planning, risk management, technical steering, validation, recommendations

Document Information

List of Contributors	
Name	Partner
Francisco Gala	ATOS
Miguel Angel Mateo Montero	ATOS
Michel Abdalla	ENS
Clément Gentilucci	FUAS
Danaja Fabcic	KU LEUVEN
Yolan Romailler / Johan Cattin	KUDELSKI
Kimmo Järvinen	UH
Norman Scaife	WALLIX
Miha Stopar	XLAB
Antonio Kung	PAB Member
Ventzi Nikov	PAB Member
Sergey Gorbunov	PAB Member
Sven Bauer	PAB Member
Vadim Lyubashevsky	PAB Member
Claire Vishik	PAB Member
Jesús García Luna	PAB Member

Document History			
Version	Date	Change editors	Changes
0.1	21/11/2019	Francisco Gala (Atos)	ToC, transcription of PAB meeting minutes, first draft
0.2	18/12/2019	Michel Abdalla (ENS)	Version for internal review
0.3	19/12/2019	Hendrik Waldner (UEDIN)	Applied review comments
0.4	19/12/2019	Michel Abdalla (ENS)	Applied review comments
1.0	20/12/2019	Diego Esteban (ATOS)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Michel Abdalla (ENS)	20/12/2019
Technical Manager	Michel Abdalla (ENS)	20/12/2019
Quality Manager	Diego Esteban (ATOS)	20/12/2019
Project Coordinator	Francisco Gala (ATOS)	20/12/2019

Table of Contents

Document Information 2
Table of Contents 4
List of Acronyms 5
Executive Summary 6
1 Introduction 7
1.1 Purpose and structure of the document 7
2 Project Advisory Meeting 25/10/2019 8
2.1 Meeting agenda and presentations summary 8
2.1.1 Welcome and Project Overview 8
2.1.2 Technical Overview 9
2.1.3 Web-analytics use-case (WALLIX) 9
2.1.4 Privacy-preserving and auditable digital currency use-case (ATOS) 9
2.1.5 Local decision making & Internet of Things use-case (KUD) 10
2.1.6 Functional Encryption Algorithm Design 11
2.1.7 Hardware Support (HW) 11
2.1.8 Functional Encryption Implementation 11
2.1.9 Session wrap-up 12
2.1.10 Ad-hoc feedback from PAB 12
3 Conclusions 13
References 14
Annexes 15
Annex I – PAB Meeting agenda 15

List of Acronyms

Abbreviation / acronym	Description
ABE	Attribute-Based Encryption
API	Application Programming Interface
AWS	Amazon Web Services
DDH	Decisional Diffie-Hellman
DMCFE	Decentralized Multi-Client Functional Encryption
EU	European Union
FE	Functional Encryption
FFmpeg	Fast Forward MPEG
GDPR	General Data Protection Regulation (Regulation 2016/679) [2]
HW	Hardware
IoT	Internet of Things
ISO	International Organization for Standardization
KYC	Know Your Customer
LWE	Learning With Errors
MPEG	Motion Picture Experts Group
P2P	Peer to Peer
PAB	Project Advisory Board
SW	Software
UC	Use-case (i.e. FENTEC prototype)
WP	Work Package
Y*x*	E.g. Y1, Y2, Y3. The year as in Project schedule; Respectively 2018, 2019, 2020

Executive Summary

This report summarizes the interactions between FENTEC and the Project Advisory Board (PAB) during the second year of the project (Y2). Most of the feedback was obtained at the yearly meeting that took place on October 25th, 2019 (online conference).

In general, the assessment from the PAB has been positive. The project seems to be on track and the objectives remain relevant.

The main recommendations for the future can be summarized as follows:

- Consider alternative routes to achieve liaison with ISO (contact provided by PAB); and
- To find balance between the technological aspects and the story behind each use case, and then keep this consistent in all of the three use cases.

1 Introduction

1.1 Purpose and structure of the document

This report summarizes the engagement of FENTEC with the Project Advisory Board (PAB) during the second year of the project. This deliverable is structured as follows:

- Section 2 presents a summary of the online meeting that took place on October 25th, 2019, and includes questions, comments, and recommendations made by the PAB members;
- Section 3 describes recommendations and next steps for the final year of FENTEC; and
- Section 4 ends the document with the main conclusions.

Additional details on the PAB members (e.g. composition, professional profiles, etc.) can be found in D2.13 [1].

2 Project Advisory Meeting 25/10/2019

FENTEC organized a half-day remote meeting to present the progress in Y2 and the current status of the project. The meeting took place on October 25th, 2019, and the PAB members provided valuable feedback, as summarized in this report.

Although the original plan was to have a face-to-face meeting, some unforeseen circumstances forced us to switch to a remote conference to which not all members were able to attend.

In a similar fashion as in Y1, Michel Abdalla (ENS, FENTEC Scientific Coordinator) and other experts working in FENTEC engaged in several bilateral conversations with some of the PAB members to cover some specific aspects of the project.

This report contains the main points discussed at the PAB meeting and the recommendations from the PAB (including additional comments via telephone calls and email exchanges).

2.1 Meeting agenda and presentations summary

Seven slots were presented, including an overview and a wrap up. The focus were the technical developments of Y2, with particular focus on the three Uses Cases (UCs). To make the best use of the time, less technical areas such as management were not covered in too much detail.

Also, the set up of the meeting had the upcoming review in mind, so some of the ideas and slides that would be presented later that year where shown to the PAB to identify areas of improvements.

PAB members were invited to interrupt at any time, but most questions were made at the end of each slot. To increase the readability of this report, all questions are transcribed at the end of each block.

The meeting agenda and the attendants can be found in Annex I – PAB Meeting agenda.

2.1.1 Welcome and Project Overview

Francisco Gala (ATOS), the Project Coordinator, presented this section. The project objectives and schedule were revisited. The work in Y2 was summarized and the current status of the project briefly explained to put everyone up to speed.

Also in this section, Kimmo Järvinen ran a short presentation with FENTEC communication and dissemination efforts, including a list of the most relevant papers published and venues attended.

The slot ended with the upcoming challenges for the remainder of the project, and the PAB made the following comments:

ISO Liaison: They were sorry we were stuck with our application for our liaison and suggested that we tried a different approach. Antonio Kung mentioned some names and contacts were provided by email shortly afterwards.

It was also mentioned that the next ISO meeting was taking place in St. Petersburg, although it was unlikely that FENTEC would be able to attend seeing the status of the application.

The conversation about standards also linked to the use cases. It was suggested to search how the pilots could be related to existing or even new standards. For instance, all those related to privacy by design.

2.1.2 Technical Overview

Next, Michel Abdalla (ENS), the Scientific Coordinator, presented a similar overview, but this time from a more technical perspective.

The main concepts related to Functional Encryption (FE) were visited again, including the potential applications and existing lines of work.

The achievements of each work package (WP) were presented at high level, these to be explained in the upcoming slots.

2.1.3 Web-analytics use-case (WALLIX)

Norman Scaife (WALLIX), WP7 leader, presented the Web Analytics UC.

The objectives of the UC were revisited, and the role of FE in this prototype was discussed.

Norman presented the system architecture and how the different elements were related. He explained the integration of DMCFE based on pairings and the implementation of primitive sub-sampling.

However, due to the time and set up limitations it was not possible to do a live demo, so a short video was played instead (this same approach would be used for the upcoming review). For this demonstration, free AWS accounts were used (e.g. in case there were privacy concerns).

The demo proved that the FE implemented in this pilot is secure and able to perform simple sampling, so all in all it meets the objectives sought.

However, there are some issues that are not completed yet. The next steps will focus on these items, namely: implementation of security checks (e.g. external attacks), preparation for performance tests and optimization, monitor memory use and experiment with new statistical analysis that could be carried out.

The results of the analytics to be carried out shortly will be used to identify areas of improvement.

In brief, the current status of the prototype is fully compliant with the design specifications (e.g. D3.1 and D7.1).

The PAB members made the following questions and comments:

The role of FE: It was recommended to point out the value of FE in this prototype and highlight why it is relevant and how value is made. The architecture is well explained but it is not that clear where the FE sits and what role it plays in protecting privacy. It was also suggested to explain the FE part a little bit better since not all the audiences, even with technical background, may fully understand it.

As a side note, Antonio Kung's (PAB) current work is related to some of these developments and he expects to cooperate with Wallix in the following months and also provide more detailed feedback on this UC.

It was also mentioned that privacy protection is something that could be interesting for ISO and FENTEC could explore this route. FENTEC replies that once we finish with our performance verification and improvements this should be definitely more relevant.

2.1.4 Privacy-preserving and auditable digital currency use-case (ATOS)

Miguel Ángel Mateo (ATOS), presented this UC.

Following the same structure as the UC before, the objectives and motivations of this pilot were presented again as a refresher for the PAB members.

Then the actual implementation of the UC was explained in full details. The blind signature scheme (Chaum) was introduced and the modifications made were explained. Also, the KP-ABE integration was briefly described.

The system architecture was shown, indicating the different roles, processes and information exchanges step by step. This was illustrated with an example on how some attributes relevant to a payment scenario could be encrypted and used in a representative transaction.

A short demo simulated a simple scenario in which one user acquires some digital currency, and depending on the attributes encrypted into the coin, it would be accepted or rejected as per the different policy settings.

To sum up, the current status of the prototype is a solid proof of concept consolidated into a simple java application and integration with FENTEC's ABE libraries.

The upcoming steps will cover the development of the functionalities for auditing, which is the other half of the UC. Once everything is working, each entity will be developed as an independent application. Also, ATOS will explore if other FE schemes can be used for auditing.

The PAB members made the following questions and comments:

Balance between technical content and background: The architecture and all the technical elements were explained well in detail, however an abstraction about what is the UC about and its benefits was missing, e.g. what does it do for the merchant, the buyer, etc. Also, the use of some general terms such as "wallet" needs to be assessed since if the context is not well defined it may be confusing for the audience.

Lastly, it was also added that it is not clear how the policies come into place and who sets them.

2.1.5 Local decision making & Internet of Things use-case (KUD)

Johan Cattin (KUD) presented the IoT (Internet of Things) UC, starting with a brief recap of the set up and motivation of this prototype in which FE is applied to video surveillance.

The architecture was presented, explaining the role of each element and the challenges they face. This architecture is translated into a demo set up in which one laptop, one camera and two Raspberry Pi are used (e.g. to act as encryptor and as gateway). The specifics of each element were described in detail, explaining the information exchanges and all the processes that take place step by step.

One of the key elements of this UC is motion detection. KUD explains the basics of the FFmpeg filters that are used and how the video stream is composed of macroblocks and motion vectors. There are some challenges in the analysis of this information, e.g. it is not easy to define a threshold to discard background noise and identify actual movement. Some of the ideas that have been tested were explained and some histograms we presented for discussion.

Lastly, the details of the set up for the demo that would take place at the review meeting were explained (i.e. this could not be done remotely for the PAB meeting).

The PAB members made the following questions and comments:

Architecture: Same as in the WALLIX UC, the architecture is simple and understandable, but it does not show where the FE sits and what is its main purpose. This should be improved for the review meeting.

There is a CEN/CENELEC group working in video surveillance that could be interested in FENTEC's work. It is noted that surveillance is a tricky topic and there are different scenarios to consider depending whether it is homeland security or civilian use.

2.1.6 Functional Encryption Algorithm Design

Michel Abdalla (ENS), WP4 leader and Scientific Coordinator presented this slot.

He started with a reminder of the three main goals of the project, these are that the FE needs to be practical, secure and applicable in different scenarios. These translate into more specific objectives, e.g. make FE suitable for our use cases, make it quantum safe and ensure that the information leakage is kept to a minimum.

The presentation continued with an overview of the specific achievements of each one of the four tasks contained in WP4, as well as some comments on the reports already delivered.

The different schemes were explained, pointing out the challenges found and how these were overcome. These include: Instantiations from DDH, Paillier, LWE, decentralized solutions, constructions with or without labels, unbounded ABE, obfuscation for pattern matching with wildcards, etc.

Another point of interest in this presentation were the publications and papers submitted by FENTEC, some of them accepted at very prestigious venues (e.g. Asiacrypt 2019, PKC 2019, etc.).

The presentation ended with the next steps and challenges ahead for the remainder of the project.

There were no specific comments nor questions related to this presentation.

2.1.7 Hardware Support (HW)

Josep Balasch (KUL), presented how HW may support FE in FENTEC. Since the focus of this PAB meeting was the UCs, this presentation was not as extensive or detailed as the others.

The presentation started with a quick overview of WP5, its objectives and how this WP relates to work in other WPs. There was a recap on the work and achievements so far, including the reports already delivered.

Then the different tasks were presented in more detail, indicating the current status of each one, the technical challenges faced, the achievements so far and what would be the next steps in each one of the tasks.

Also, it was noted that a demo would be carried out during the review.

There were no specific comments nor questions related to this presentation.

2.1.8 Functional Encryption Implementation

Miha Stopar (XLAB), WP6 leader, presented FE schemes implemented so far. Same as with the HW presentation, this was just a quick overview. The links to the two libraries were provided and the papers used for these implementations where listed.

XLAB presented the showcases they have developed to illustrate what these schemes can do and help other developers to implement FE.

There were no specific comments nor questions related to this presentation.

2.1.9 Session wrap-up

PAB members were generally satisfied with the achievements and current status of the project.

During the wrap up, they added:

- The architectures are generally good and Antonio (PAB) volunteered to help us improve them further
- Fine grained policy management is very important if there is data available. We should take this into account
- It is uncertain that we will be able to participate in standardization activities, but we should keep pushing forward
- The next PAB meeting is tentatively set to Q2 2020

2.1.10 Ad-hoc feedback from PAB

The slides used in the meeting were shared with the PAB and they were invited to come back with additional questions, particularly those that were not able to attend. No additional feedback was received.

3 Conclusions

The interactions with the PAB during the second year of the project have been very positive, with the PAB actively supporting the FENTEC project. Besides the yearly meeting, additional interaction has been taken place by email and telephone conversations, mainly with the Scientific Coordinator. These interactions are to be maintained and strengthened for the last year of the project.

The main recommendations for the future are related to finding the balance between the technical and non-technical aspects of FENTEC, making sure that the background of the use cases is clear, along with their benefits, making clear where the Functional Encryption sits and what are the advantages of the innovative approach of the project.

References

[1] D2.13 Project Advisory Board Workshop Report Y1. FENTEC Consortium, December 2018

[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Annexes

Annex I – PAB Meeting agenda

Date: 25 October 2019
Time: 9:30
Location: Online

Attendees:

Francisco Gala	ATOS
Miguel Angel Mateo Montero	ATOS
Michel Abdalla	ENS
Clément Gentilucci	FUAS
Josep Balasch	KU LEUVEN
Danaja Fabcic	KU LEUVEN
Wim Vandevelde	KU LEUVEN
Yolan Romailler	KUD
Johan Cattin	KUD
Hendrik Waldner	UEDIN
Kimmo Järvinen	UH
Norman Scaife	WALLIX
Miha Stopar	XLAB
Sergey Gorbunov	AB Member
Antonio Kung	AB Member
Ventzi Nikov	AB Member
Claire Vishik	AB Member (Excused)

Main objectives

- Overview of FENTEC: objectives, organization, key personnel, approach, WP structure, etc.
- Presentation of the work carried out so far
- Use Case Updates
- Next steps and work plan for Y3

AGENDA 25 October 2019

Time	Topic	Presenter
09:30-09:40	Welcome, quick round of presentations	ATOS
09:40-09:50	**FENTEC OVERVIEW** • Project summary • Objectives, outputs • Project work so far	ATOS
09:50-10:00	**TECHNICAL OVERVIEW** • Brief introduction • Overview of main results • Expected impact	ENS
10:00-10:45	**USE CASES** • Data collection (WALLIX) • Digital Currency (ATOS) • IoT (KUD)	WALLIX ATOS KUD
10:45-11:00	***BREAK***	
11:00-11:15	**FE ALGORITHMS** • Results • Next steps	ENS
11:15-11:25	**HW SUPPORT** • Results • Next steps	KU LEUVEN UH
11:25-11:40	**SW IMPLEMENTATION** • C and Go functional encryption library • Machine learning classification on encrypted data • Next steps	XLAB
11:40 – 12:10	**WRAP UP** • Evaluation of project so far • Recommendations and next steps (e.g. D2.13)	ALL