D2.13 Project Advisory Board Workshop Report Y1

Document Identification			
Status	Final	**Due Date**	31/12/2018
Version	1.0	**Submission Date**	18/12/2018

Related WP	WP2	**Document Reference**	D2.13
Related Deliverable(s)	D2.14, D2.15	**Dissemination Level (*)**	PU
Lead Participant	ENS	**Lead Author**	Michel Abdalla
Contributors	Francisco Gala (ATOS)	**Reviewers**	Clément Gentilucci (FUAS)
			Hendrik Waldner (UEDIN)

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

This document is issued within the frame and for the purpose of the FENTEC project. This project has received funding from the European Union's Horizon2020 under Grant Agreement No. 780108. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

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	KUDELSKI
Kimmo Järvinen	UH
Norman Scaife	WALLIX
Miha Stopar	XLAB
Sven Bauer	PAB Member
Sergey Gorbunov	PAB Member
Vadim Lyubashevsky	PAB Member

Document History			
Version	Date	Change editors	Changes
0.1	26/11/2018	Francisco Gala (Atos)	ToC, transcription of PAB meeting minutes, first draft
0.2	29/11/2018	Michel Abdalla (ENS)	Revised comments about the PAB questions, added missing bios
0.3	17/12/2018	Michel Abdalla (ENS)	Version for reviewing
0.4	17/12/2018	Michel Abdalla (ENS)	Addressed reviewer comments
0.5	18/12/2018	Kimmo Järvinen (UH)	Updates to Section 3.1.8
0.6	18/12/2018	Michel Abdalla (ENS)	Additional feedback from PAB
1.0	18/12/2018	Diego Esteban (ATOS)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Michel Abdalla (ENS)	18/12/2018
Technical Manager	Michel Abdalla (ENS)	18/12/2018
Quality Manager	Diego Esteban (ATOS)	18/12/2018
Project Coordinator	Francisco Gala (ATOS)	18/12/2018

Table of Contents

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
GDPR	General Data Protection Regulation (Regulation 2016/679 [3])
HW	Hardware
IoT	Internet of Things
KYC	Know Your Customer
LWE	Learning With Errors
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 mainly summarizes the discussions held during the online meeting that took place on the 26th of November 2018 and in which the Consortium presented FENTEC to the Project Advisory Board (PAB), including the work done so far and upcoming challenges.

Overall, the PAB response has been positive: The project seems to have clear objectives and to be on the right track and they are looking forward to the more tangible results expected for Y2.

The main recommendations for the future are:

- to consider a liaison with SC27 regarding standardization;
- to account for the problem of censorship in the transactions in the digital-coin use case;
- to avoid the use of Gaussian sampling when possible due to their susceptibility to side-channel attacks;
- to clarify the common ground that links the different use cases to better justify the use of functional encryption in these use cases;
- to clearly indicate how functional encryption can provide advantages for KYC, GDPR, or generic ethical considerations;
- to explore the connections between SW and HW implementation; and
- to continue making the project results available on GitHub since this seems to be a great asset for dissemination.

1 Introduction

1.1 Purpose of the document

This report summarizes the engagement of FENTEC with the Project Advisory Board (PAB) during the first year of the project. This deliverable includes:

- Background information on the PAB members. Composition, professional profiles and changes to the nominees during the proposal stage
- Summary of the online meeting that took place on the 26th of November of 2016. In this meeting, the PAB and the Consortium were formally introduced and the current status of the Project, in terms of work done so far and upcoming tasks, was discussed
- Recommendations and next steps for Y2.

1.2 Structure of the document

The remaining three sections of D2.13 are structured as follows:

- Section 2 provides some background on the foundation of the PAB and its current composition.
- Section 3 summarizes the discussions that took place during the PAB online meeting (26/11/2018).
- Section 4 closes the document with a brief conclusion.

2 Project Advisory Board

In FENTEC Grant Agreement [1], Task T2.5 "FENTEC Project Advisory Board" sets the requirement of a Project Advisory Board (PAB), which consists of "*6 experts in security and privacy from Bosch, NXP, Giesecke & Devrient, Trialog, Zenith Analytics, Intel Corporation UK Ltd*". Also, the Grant Agreement sets a minimum of three formal meetings, of which the first one will be online.

This section presents FENTEC PAB, its members and the process to establish the board, including some changes that were required due to the availability of the members that were originally nominated during the proposal stage and at the signature of the Grant Agreement.

2.1 Establishment of the Project Advisory Board

Starting with the experts that had supported FENTEC during the proposal stage (e.g. by signing letters of intertest) the Consortium launched a first round of contacts with potential PAB members in February 2018.

The request was accompanied by a short document that outlined the purpose of the PAB and roles and responsibilities of the PAB (see Annex I – Invitation to FENTEC PAB).

Due to personal and professional changes, some of the experts could not commit to the Project any longer. The Consortium drafted a list of potential substitutes and these were contacted in decreasing order of preference.

To increase the expertise of the PAB, it was decided to increase the number of members from six to seven.

2.2 Current composition of the Project Advisory Board

The current composition of the PAB, including a short bio, is as follows:

Dr. Antonio Kung has more than 30-year experience on embedded systems and ICT systems. He co-founded Trialog in 1987 where he acts as CEO. He has coordinated several collaborative projects in the area of security and privacy (PRECIOSA, PRIPARE, PARIS). He is active in standardization (editor of ISO/IEC 27550 privacy engineering, rapporteur of two study periods: privacy guidelines for the IoT, privacy in smart cities). He is a member of the IPEN community, responsible for a wiki on privacy standards (ipen.trialog.com). He holds a Master's degree from Harvard University, USA and an engineering degree from Ecole Centrale Paris, France.

Dr. Claire Vishik's work focuses on hardware security, trusted computing, privacy enhancing technologies, some aspects of encryption and related policy issues. Claire is a member of the Permanent Stakeholders Group of ENISA, is active in standards development and is on the Board of Directors of the Trusted Computing Group and on the Council of the Information Security Forum. Claire is active in developing R&D strategies for security and privacy, through organizations like Cybersecurity Research Alliance and strategy efforts in the EU, US and other countries. She is an

advisor to a number of R&D projects and initiatives including IPASco, PUFFIN, a cryptography program at the University of Bristol, and many others.

Dr. Jesus Luna is currently a Security Architect in Bosch, at Corporate Sector Information Systems & Services - Governance Security (CI/GS) department. Previously Jesus was the Research Director of the Cloud Security Alliance (Europe) where his main responsibilities included the internal scientific/technical management of CSA's funded projects. Jesus obtained his PhD degree in Computer Architecture from the Technical University of Catalonia (2008). Since 2003, Jesus is also affiliated with the Technische Universität of Darmstadt, Germany. His main research interests are security quantification, cloud security, and security policies.

Prof. Sergey Gorbunov is an Assistant Professor at the University of Waterloo and Head of Cryptography at Algorand. His research interests range from foundational cryptography to design of secure large-scale systems, computer networks, protocols and blockchains. He received PhD from MIT in '15 where he was the recipient of the Microsoft PhD fellowship. His dissertation was on building advanced cryptographic protocols using lattice-based cryptography for which he received Sprowl's Doctoral Thesis Prize for best PhD thesis in CS at MIT. He was also the founder and CTO of StealthMine, and spent some time at IBM T.J. Watson Research Centre.

Dr. Sven Bauer studied mathematics at the University of Marburg (Germany) and earned a PhD from the University of Aberdeen (UK). He joined Giesecke & Devrient in 2001 as a cryptologist. Since then he has been working on secure implementations of cryptographic algorithms on smart cards.

Dr. Vadim Lyubashevsky is a cryptographer in the Security group of the Cognitive Computing & Industry Solutions department at IBM Research, Zurich. His research focus is on designing data protection protocols with improved security and is supported by an ERC starting research grant FELICITY (Foundations of Efficient Lattice Cryptography), the goal of which is to design practical public key cryptographic schemes that will remain secure even in the presence of quantum computers.

Dr. Ventzislav Nikov received his Ph.D. from Technical University Eindhoven, The Netherlands in 2005. From 2000 to 2002, he was a Security Expert and an Architect with ACUNIA, Leuven, Belgium and from 2004 he has been with Philips and then NXP Semiconductors, Leuven, Belgium as a Principal Security Researcher and an Architect. His research focuses on multi-party computation, block ciphers and side-channel resistant techniques. He published over 50 research papers, filed 20 patents.

3 Project Advisory Meeting 26/11/2018

On the 26th of November of 2018 FENTEC organized a half-day online meeting with the main objective of presenting the Project to the PAB and obtain valuable feedback from the experts.

Unfortunately, due to numerous agenda conflicts and some last-minute cancellations (which forced a short-notice re-scheduling of the meeting originally set for 19/11/2018), only three out of seven PAB members were able to attend. To cover for this, Michel Abdalla (FENTEC Scientific Coordinator) contacted separately the remaining PAB members to inform them about the project status and its main challenges.

This section contains a summary of the topics that were presented at the PAB meeting and at the end it also synthetizes the discussions and recommendations from the PAB members (both during the meeting and individual telephone calls).

3.1 Meeting agenda and presentations summary

The meeting was divided into eight slots in which members of the Consortium presented different lines of work in FENTEC.

Most questions were asked at the end of each presentation, however for the sake of clarity, the transcript of questions and answers are presented in one single section.

The meeting agenda, including the attendants, can be found in Annex II – PAB Meeting agenda.

3.1.1 Welcome and Project Overview

This section was presented by Francisco Gala (ATOS), the Project Coordinator.

The meeting started with a brief introduction of the Consortium representatives and the PAB members, who were able to briefly present their expertise and field of work.

This short presentation included the main objectives of the meeting and an overview of the agenda and the upcoming slots.

Next, the three main objectives of FENTEC were discussed (develop Functional Encryption, implement into an API, create three prototypes) along with a high-level overview of the project.

The presentation continued with the work done so far (e.g. deliverables already presented, or under production) and closed with the main challenges for the second year of FENTEC.

3.1.2 Technical Overview

Next, the conversation moved into technical overview of the Project. This slot was presented by Michel Abdalla (ENS), the Scientific Coordinator.

The concept of Functional Encryption (FE) was introduced, along with some potential applications, advantages and current lines of work.

The Project objectives, which had already been introduced, were discussed in more details. This included the balance among expressiveness, security and efficiency, issues related to inefficient

primitives and potential hardware (HW) support, and the ambition of FENTEC to deliver products as close to the market as possible.

This block ended with a high-level presentation on how the work is distributed into Work Packages (WP) and the interrelationships among all of them.

3.1.3 Web-analytics use-case (WALLIX)

This slot was presented by Norman Scaife (WALLIX), who is the WP7 leader and the main contact point for the Web Analytics use-case (UC).

The motivation for the selection of this use case was discussed. There is a legitimate interest in obtaining this information, not only because of an attractive market potential but also as a path to improve system efficiency. However, there are some strong controversies and the privacy of clients must be preserved. There are also some limitations, but FE is a promising technology that could be deployed in this field.

This UC considers the interface with Amazon AWS servers (command line) in which FE could address the existing problems by keeping the data private while removing the need for a trusted server.

The implementation considers the integration of FENTEC libraries (Distributed Multi-Client FE) into AWS according to the specifications, then follow up with testing and performance measurements (e.g. including HW acceleration).

So far, the specifications have been gathered (e.g. D7.1 [2]) and the implementation has already started (early stages).

The first prototype is expected later in Y2 (Oct 2019).

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

This presentation was made by Miguel Ángel Mateo (ATOS), who is the main contact point of the digital currency UC.

The three main challenges of this UC were introduced: preserve privacy, minimize the amount of information required by each transaction, ensure the veracity of each operation. Since Atos is a world leader in electronic transactions, emerging technologies with potential application in this field are of great interest for the company.

Taler, which is based on Chaum principles, has been chosen as the platform on which the digital currency will be developed. The main actors and the relationships among them were also discussed.

This UC aims at developing two scenarios, one oriented at controlling the attributes of the coin/the transaction (e.g. similar to restaurant cards/checks already available in the market) and another one in which auditors would be able to obtain, depending on each situation, a tightly controlled amount of information. Each scenario exemplified and competed with a list of attributes that could apply in each case.

3.1.5 Local decision making & Internet of Things use-case (KUDELSKI)

This slot was presented by Yolan Romailler (KUD), who is the main contact point of IoT (Internet of Things) UC.

As with the other prototypes, the motivation behind this UC was discussed: the increase in the number of IoT devices, the current set-ups, the limitations, known problems, and how FE could be a potential

solution in this environment. Some examples, such as smart metering and video streaming (FENTEC UC), were introduced.

The UC focuses on a local decision making at the gateway level, therefore maintaining end-to-end encryption and thus saving bandwidth (which may be scarce in an IoT environment). Some alternatives were presented, but in the end justifying the ambition of using FE in this prototype in which motion vectors need to be assessed.

The implementation will be based in FFmpeg and it will be divided in three phases. Once implemented, the prototype will be tested in a controlled environment and then the performance will be assessed.

As with the other UC, the specifications have been published (e.g. D7.1 [2]) and the first version is expected by October 2019 (at least up to phase 1 - split motion-vectors and local decision making at the gateway level).

3.1.6 Legal and ethical aspects of FENTEC

This presentation took place after a short break that was also used to change the conference bridge due to some technical problems. Danaja Fabcic (KU Leuven) explained the relevance of the legal and ethical aspects related to FENTEC.

The main concepts, such as dual use and misuse, and the GDPR, were introduced to the PAB. Additionally, specific legislation that may affect each use-case was briefly presented. The aim of FENTEC is to have final products that are compliant with all regulations.

Legal and ethical management are a joint effort in FENTEC; KU Leuven takes the lead with two dedicated tasks (setting the requirements and monitoring compliance), plus the role of the Ethical Manager. When needed, KU Leuven Ethics Committee will be consulted.

There are some challenges that must be taken into account. For example, high-level regulations may be too vague and not easy to translate/adapt for the given use-cases. Also, the normative fragmentation due to different rules in EU member states, along with possible changes in regulation (e.g. the GDPR that came into place some months ago), are to be considered for the duration of the Project.

Lastly, the IoT use-case was presented in more detail and used as an example of all the legal implications that fall behind and covering all the key ethical and legal aspects related to this UC. Examples included the specific interpretation of Belgian Law when it comes to the use of cameras in public areas, the dilemma if people can be recognised when the stream is encrypted, the application of the “privacy by design” principle, etc.

3.1.7 Functional Encryption Algorithm Design

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

The development of new FE schemes that are practical and ready for real applications (e.g. FENTEC three prototypes) is one of the core objectives of the Project. Along with this goal, FENTEC will also work in quantum-safe FE and in reducing potential information leakage.

The work towards new FE is concentrated in FENTEC WP4 and split into four tasks: application-specific FE, expressive FE, quantum-safe FE and a complimentary task dedicated to information leakage and countermeasures.

The application-specific FE will study existing schemes and evaluate if they meet the requirements for the use-cases. When needed, new FE schemes will be developed or existing schemes will be updated

or improved. The schemes that are being used at the moment include: “Multi-Input Inner-Product Encryption Without Pairings” and “Distributed / Decentralized Multi-Client Inner-Product Encryption” (all for web analytics UC); and “Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding” (IoT UC).

The second task of this WP is to make FE useful for a wider range of applications by considering trade-offs between efficiency and expressiveness. This is due to the fact that FE schemes for general functions such as polynomial-size circuits are rather theoretical and therefore of limited practical interest. Some of the work already in progress includes “Unbounded ABE via Bilinear Entropy Expansion”; and “Obfuscation for Pattern Matching with Wildcards from Knowledge Assumptions”.

The third task considers the challenge that quantum computing may pose to FE schemes. The goal of this task is to work on lattice-based FE schemes and investigate how to improve their efficiency. Work in this area includes “Multi-Input Inner-Product Encryption Without Pairings”; and “Decentralized Multi-Client Inner-Product Encryption from LWE”.

The last task in this WP analyses the potential information leakage in the different schemes (e.g. combining Attribute Based Encryption and FE) and the potential deployment of countermeasures.

The focus in the upcoming year will be on improving security guarantees, trying to extend existing results to quadratic functions and low-degree polynomials, building lattice-base alternatives, and restricting the decryption capabilities of keys to minimize information leakage.

3.1.8 Hardware Support

Kimmo Järvinen (UH), WP2 leader and one of the main contributors to WP5, presented how FENTEC supports FE with HW.

WP5 already worked on Trust Analysis considering HW requirements and selected HW platforms. D5.1 described a general computing platform as an abstraction of specific platforms that will be used) in WP5 (server/cloud, embedded, and end-node environments) and described security and trust analysis. The attacks considered in WP5 are passive side channel and active fault attacks.

T5.2 studies HW implementation of FE schemes and aims to maximize the efficiency of implementations by optimally utilizing the features of the target platform (e.g., to accelerate the performance of FE implementations with FPGA-based coprocessors). Side-channel or fault attacks are mostly out of the scope of this task, with the exception of attacks that can be done over the network (e.g., the implementation must be constant time to protect against timing attacks).

T5.3 considers platforms that include an element that can be trusted (e.g. trust anchor) and studies how it can be utilized in implementations of FE schemes.

T5.4 considers platforms, which lack a trusted element and are susceptible to implementation attacks. The focus is to ensure that all components are hardened against side channel and fault attacks.

The HW platforms considered so far are: Xilinx Ultrascale+ ZCU102, which helps to accelerate algorithms for server/cloud use cases; Hikey 960, which is useful for embedded environments and for relying on TrustZone; and Sakura-X, which will be used in T5.5 for side-channel attack evaluations.

Work has been divided so that KUL focuses on (R)LWE FE schemes. The first results on Saber on ARM and on efficient polynomial multiplication on ARM processors were published in CHES 2018.

UH focuses on FE schemes based on modular arithmetic with large integers (e.g., Paillier and Pairing-based schemes), and is currently working on a single-core prototype on FPGA that will be extended to multi-core architecture during the second project year.

3.1.9 Functional Encryption Implementation

Miha Stopar (XLAB), WP6 leader, presented the implementation of FE schemes.

The objectives of this WP are to check existing FE libraries, choose underlying libraries (e.g. for pairings and lattices), and implement four schemes in two different languages.

Fully-fledged libraries for FE are not yet available. The only resources available in Github are simple prototypes with one single scheme.

FENTEC has released one library in Go (GoFE), which has been presented at IFIP. The C version is in the process of being released (CiFEr).

WP6 has been also providing building blocks such as pairing libraries in GO (forked BN256 to support hashing to G1, G2), and C (AMCL). Since lattice libraries were not available, these had to be developed from scratch. The output of this WP also supports vectors and matrices operations, discrete log computation and samplers (including uniform and gaussian)

So far, the implemented schemes include: Simple inner-product (DDH, LWE); Fully secure inner-product (DDH, LWE, R-LWE, Paillier); Multi-input inner-product (DDH, Fully-secure DDH); and Quadratic multi-variate polynomials.

Current work in progress focuses on BE and DMCFE schemes. A CiFEr library will be released and work on further schemes will carry on. Performance improvement will also be addressed in Y2. E.g. performance is better when based on RLWE, but what is still missing are the security proofs that existing FE schemes remain secure in this RLWE setting.

3.1.10 Questions and session wrap-up

PAB members enquired on several issues during the meeting. Their most important questions (e.g. small clarifications are omitted) and the answers are transcribed below:

Q: On digital coins: One of the main advantages of a decentralized cryptocurrency is the ability to prevent censorship of individual transactions. This is achieved via a combination of P2P protocols and decentralized consensus. In the architecture shown in the slides, can the central exchange censor individual payments?

A: The current design of the pilot does not take into account the problem of censorship on the transactions.

A: (sent via a follow up email): The Taler payment platform does not keep information regarding which coins have been delivered to which customer. To achieve this, the exchange server uses blind signatures to deliver digital coins to customers (i.e., customers' wallets). More information in https://taler.net/en/faq.html.

Moreover, when a customer pays a merchant, there is no private information involved in the payment. Once the merchant receives the coins and requests the Exchange server to check that there is no double spending, the exchange server does not know any data about the customer. In that way, even though the exchange server could censor a payment transaction, this decision would not be based on the customer data or nature.

Finally, independently of whether or not there is an incentive for the exchange server to censor transactions, we will investigate ways of preventing any type of transaction censorship by design.

Q: On implementation of FE: which implementations are using Gaussian sampling? Do they require trapdoor sampling?

A: Currently, the lattice-based schemes under consideration use Gaussian sampling. The Paillier based instantiation also seems to require it. However, generally speaking, Guassian sampling is not required in non-lattice-based schemes.

PAB: It is better to avoid the use of Gaussian sampling in lattice-based schemes if trapdoor sampling is not required. Vadim Lyubashevsky agreed to be contacted if needed for lattice-related questions.

Q: On implementation: How are SW and HW connected at implementation?

A: It is envisaged to have a synchronization/co-design in WP5 by taking implementations from WP6 into account (e.g. using reconfigurable FPGA for multi-core environments). There are high level plans but FENTEC is still working on the details. Results are expected for Y2.

Before closing the meeting, the PAB members were asked their opinion on FENTEC, more precisely on the overall set up of the Project (e.g. roles, distribution for organization of work), the objectives set, the results so far and the upcoming challenges.

The response was unanimously positive. The PAB members think that FENTEC is an interesting project, with clear objectives and that seems to be on track. They expressed their shared expectations of seeing FE leaving the theoretical/academic realm and start being applied to specific use cases.

3.1.11 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. These interactions were managed by Michel Abdalla (ENS).

The summary of this additional feedback is as follows:

Q: Will the entire project remain open-source? You mentioned some commercialization efforts ...

A: Go is Apache License 2, C is dual license GNU LGPL v3 and GNU GPL v2. We also remark that these issues will be fully addressed in the exploitation plan (Y2).

Dr. Antonio Kung indicated that FENTEC has a great potential to create an avenue of cryptography, since the project includes a number of use cases and demonstrating the feasibility of FE in these use cases will be key to the success of FE. He also indicated that the smart metering could be an interesting use case due to its requirement for end-to-end encryption.

Regarding standardization, Dr. Kung also recommended to consider a liaison with SC27. More specifically, he made the following suggestions

- Socializing the concept of FE: This can be done in WG2 but also in WG4 and WG5 where the impact of a FE-based encryption on architecture and on trust could be pointed out (e.g. WG4 has a study on device security);
- Proposing a study period on FE (based on results from FENTEC); and
- Possibly proposing a technical report.

Dr. Kung additionally mentioned that the availability of a GitHub with existing FE encryption schemes is a great asset for dissemination and applauded this approach.

Dr. Claire Vishik indicated that she appreciates the work done within the FENTEC project and made the following suggestions:

- Although it is useful to have different use cases, it would be helpful to provide the common ground that links them in order to better justify the use of functional encryption in these use cases.
- More specific approaches would be appreciated. For instance, the current slides do not clearly indicate how functional encryption can provide advantages for KYC, GDPR, or generic ethical considerations. There are definitely easy-to-see benefits, but it would make sense to explain them better.

Finally, both Dr. Jose Luna Garcia and Dr. Ventzislav Nikov indicated that they were happy to see that the project seems to be progressing well, but that they did not have any further comments.

4 Conclusions

The interactions with the PAB have been very positive. The PAB members have been very helpful and supportive of FENTEC. Although due to some unforeseen circumstances only three members were able to attend, the entire PAB was able to offer additional feedback via ad-hoc conversations with the Scientific Coordinator. For the future, it is envisaged to maintain this close relationship with the PAB members, both individually and with the PAB as a whole.

The online meeting was a very good opportunity for FENTEC to self-assess progress and start wrapping up the work done so far in Y1, and also to present the first results and discuss the upcoming challenges with the PAB experts. The shared opinion of the PAB was that the Project line of work is very interesting and covers quite challenging topics, and that it is well organized and progressing on track. Finally, the PAB also shared their expectations on seeing FE finally brought closer to real-life applications.

References

[1] FENTEC Consortium Agreement (No. 780108). FENTEC- EC, November 2017

[2] D7.1 Preliminary Specification of FENTEC Prototypes. FENTEC Consortium, September 2018

[3] General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Annexes

Annex I – Invitation to FENTEC PAB

1. Purpose

FENTEC is a H2020 project, which started in January 2018. Its main objectives are:

- to design novel functional encryption systems for scenarios with varying functional, security, hardware, and software requirements;
- to implement a unified highly optimized cryptographic API of functional encryption schemes for present and future applications;
- to validate its results and demonstrate their benefits through prototyping; and
- to disseminate the results achieved and pave the way for their commercialization.

This document describes the context in which the ***FENTEC*** Advisory Board (AB) members will intervene as well as the practical arrangements for collaboration.

2. Objective of the Advisory Board

The main role of the AB is to ensure that the Consortium appropriately analyses/addresses the influence of external factors on ***FENTEC***.

The tasks of the AB as a whole are to:

- Provide technical, ethical and legal guidance to the project
- Provide input and feedback on the achievement of the ***FENTEC*** objectives and results
- Advise on links with relevant interest groups outside ***FENTEC***
- Propose and encourage the potential interactions of the project with other projects, initiatives and activities not previously identified by the Consortium, and support ***FENTEC*** in this attempt in leveraging their own network(s) whenever possible.

3. Roles and responsibilities of the Advisory Board members

The Advisory Board members commit to the following tasks:

- To attend the ***FENTEC*** Advisory Board meetings and teleconferences scheduled to support the project scientific coordination: we estimate to have one 1-day AB meeting/teleconference a year;
- To read, analyze, and make recommendations on selected ***FENTEC*** deliverables; and
- To act as an ambassador to help optimizing impact and enhancing the sustainability of the results.

The Chair of the Advisory Board will prepare, together with the Project Director and Technical Coordinator, the Advisory Board meetings, and will be responsible for formulating the strategic recommendations and advice of the Advisory Board to the consortium.

Potentially, AB members will be invited to attend selected project meetings and workshops, depending on the respective expertise and availability of the AB members.

The total effort is estimated on an average of 2-3 days per year.

4. Financial provisions

The Advisory Board member will contribute to the AB as described above **without payment for the time and effort spent**. The project holds a dedicated budget to cover the travel and subsistence costs for attending meetings and workshops. This budget is based on:

- Economy class flight or train ticket between the Advisory Board member's home locations and the meeting places;
- Local transport between the airport and the meeting places; and
- Hotel rooms recommended by the project.

Lunches and dinners will be organized with the project partners and will be covered by the project.

In the ***FENTEC*** project, ENS/CNRS manages this budget and will liaise with the AB members for organizing their travels and managing the expense claims and related reimbursement.

5. Confidentiality

In the case that ***FENTEC*** AB members are given access to confidential information, a specific non-disclosure agreement will rule access to such information.

Annex II – PAB Meeting agenda

Project Advisory Board 2018

Date: 26 November 2018
Time: 10:00
Location: Online (connection details at the end)

Attendees:

Francisco Gala	ATOS
Miguel Angel Mateo Montero	ATOS
Michel Abdalla	ENS
Clément Gentilucci	FUAS *(Excused)*
Sebastian Gajek	FUAS *(Excused)*
Angshuman Karmakar	KU LEUVEN
Jose Maria Bermudo Mera	KU LEUVEN *(Excused)*
Danaja Fabcic	KU LEUVEN
Wim Vandevelde	KU LEUVEN *(Excused)*
Yolan Romailler	KUD
Hendrik Waldner	UEDIN
Kimmo Järvinen	UH
Norman Scaife	WALLIX
Miha Stopar	XLAB
Sven Bauer	Giesecke+Devrient Mobile Security (PAB Member)
Sergey Gorbunov	University of Waterloo (PAB Member)
Vadim Lyubashevsky	IBM Research (PAB Member)

Main objectives

- Formal introduction between the Consortium and the PAB member
- Overview of FENTEC: objectives, organization, key personnel, approach, WP structure, etc.
- Presentation of the work carried out so far
- Next steps and work plan for Y2

AGENDA 26 November 2018

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