



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780108. Any dissemination of results here presented reflects only the consortium view.

## CONTENT

- [1. Current Status](#)
- [2. Implementation Status](#)
- [3. Use cases Status](#)
- [4. New Scientific papers](#)
- [5. Events](#)
- [6. FENTEC goes social](#)
- [7. Next Steps](#)

## JOIN US!

Subscribe

## FOLLOW US!



Twitter



LinkedIn



Last post!



Website

## Functional ENcryption TECnologies

After 17 months of hard work, **FENTEC** has successfully passed the first review of the project. The Review was hosted in Leuven the 31<sup>st</sup> of January 2019 and representatives from all the consortium partners were present.

## CURRENT STATUS OF THE PROJECT

At this stage of the project, the Consortium has identified several key assets with potential market value. In order to define a sustainable strategy to develop and exploit these assets, an **Exploitation Board** has been created. The Exploitation Board is composed by 7 exploitation specialists from several partners and they are already working on the **deep analysis of the technical results** of FENTEC project. With a roadmap already defined, next steps will be focused on the analysis of barriers and enablers, the definition of individual and joint exploitation vehicles and IPR considerations.

# IMPLEMENTATION STATUS

While the majority of the FENTEC toolset has been implemented in the first year of the project, the Consortium added some **additional schemes** (mostly attribute-based encryption), provided some **API optimizations** and **performance tweaks** in the first half of the second year.

Furthermore, **three Functional Encryption showcases** have been provided and made open-source as reference projects. These aim to help potential adopters to use the FENTEC toolset:



Privacy-Friendly Prediction of Cardiovascular Diseases.



A generation of the traffic heatmap for London Underground solely on the encrypted data.



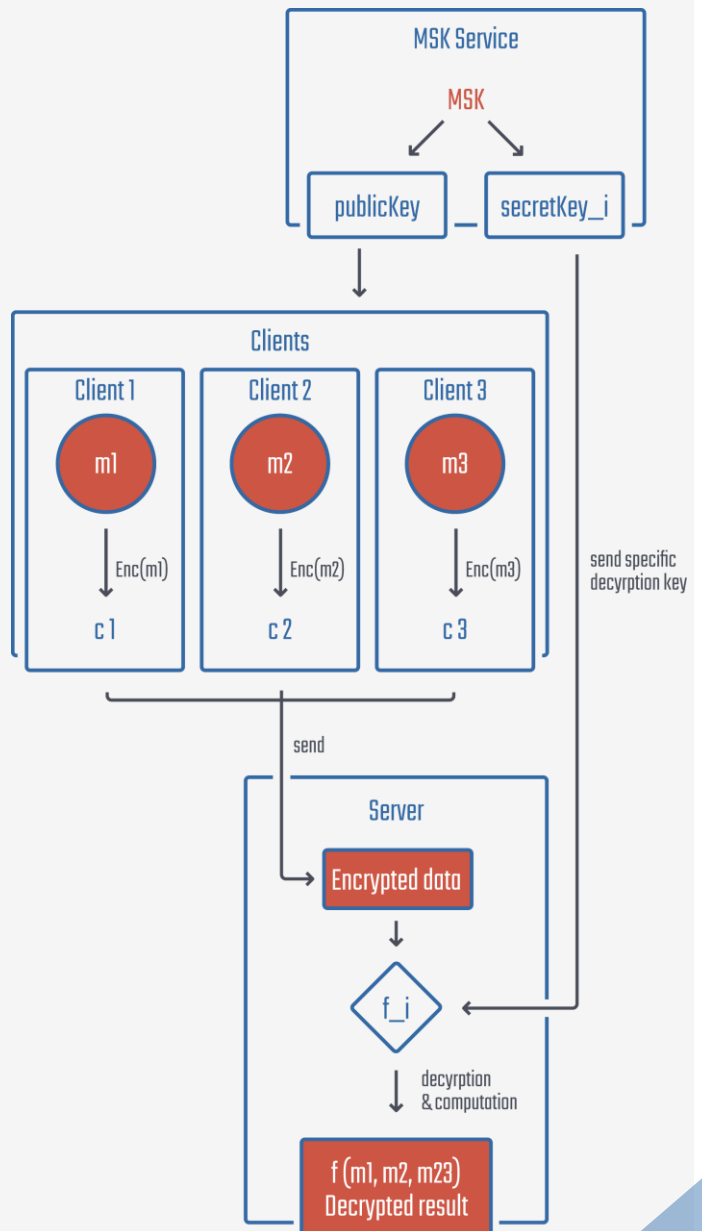
How to manage access to clinical history files.

# USES CASES STATUS

## PRIVACY-PRESERVING STATISTICAL ANALYSIS

### Overview of Current work

Work on the **WALLIX** use case is proceeding according to plan. The preliminary framework has been completed including updates to the server code extracted from **WALLIX's DataPeps product** and code from the **Awless open source tool for AWS management**. The preliminary DMCFE protocol based around pairings has been successfully integrated into the framework giving an initial design which yields average counts of accesses to AWS endpoints. Initial performance results are within acceptable bounds.



A **primitive sampling mechanism has been devised** and implemented. This involved revising the design in previous FENTEC documents slightly. In order to implement the selection phase, the cryptographic initialization is now deferred until after the statistics gathering phase has completed. This does not impact the cryptography in any way but does require a **new redistribution phase** (sample selection). Sampling is currently performed on a random basis but there is provision for using locally-computed estimates of significance in order to provide ranking based on significance.

Finally, by encoding an encryption of the squares of counts alongside the encrypted counts, WALLIX are able to provide a naive computation of the variance of statistical counts. Although this computation is essentially for free (wrapping the communications with the counts does not lead to any communications overheads), **the naive computation is not numerically stable** for small values of variance. A more stable computation is possible but would require yet another additional redistribution phase.

## Challenges

The current effort is in preparing for the **testing and performance evaluation** which will be required later in Y2. The test code is about half-finished with the server test code completed and the client test code under way. A similar effort will be required for the **performance analysis**.

There will also be **an update to the cryptography** when the new **DMCFE protocol**, not based on pairings, becomes available. Since all DMCFE protocols are of very similar structure and since the use case framework has been designed to accommodate multiple protocols, incorporating new protocols should be very easy.

*"The current effort is in preparing for the testing and performance evaluation"*

## Next steps

The next tasks will include **completing the test code** and **doing some more detailed performance analysis**.

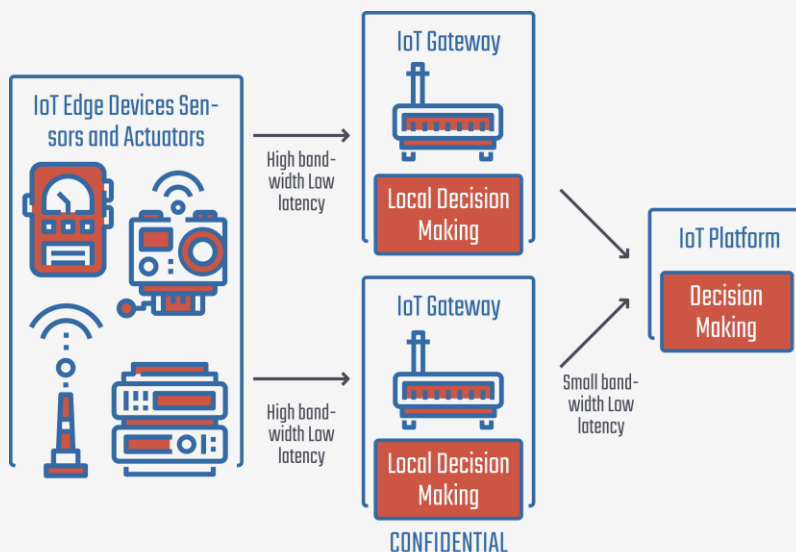
**The main target for Y2** will be a demonstration of the polling technique for the next project review in November.

## USES CASES STATUS

### MOTION DETECTION AND LOCAL DECISION MAKING

#### Overview of Current work

**Kudelski Security** are working on the **extraction of the motion vectors out** of a video stream and on the processing of a motion flow at the gateway level to detect motion using simple functions. See below for an example created using our current prototype.

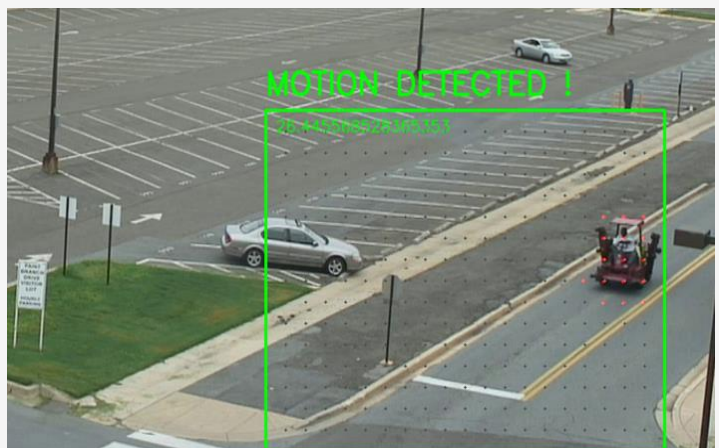


#### Challenges

The video processing is CPU intensive and the data **Kudelski Security** have to process is larger than expected even for a simple video file. Adding the layer of **Functional Encryption** on top of it might very well degrade the performance even further.

#### Next steps

Implementing the whole prototype chain, from video preprocessing and encryption, to gateway level local decision making, to the final backend system. Effectively this means finishing phase 1 of our prototype. **Kudelski Security** also have planned to experiment with the mpeg motion vectors instead of the OpenCV motion flows we are currently using. Next, the company will look at adding the encryption layer as planned for phase.



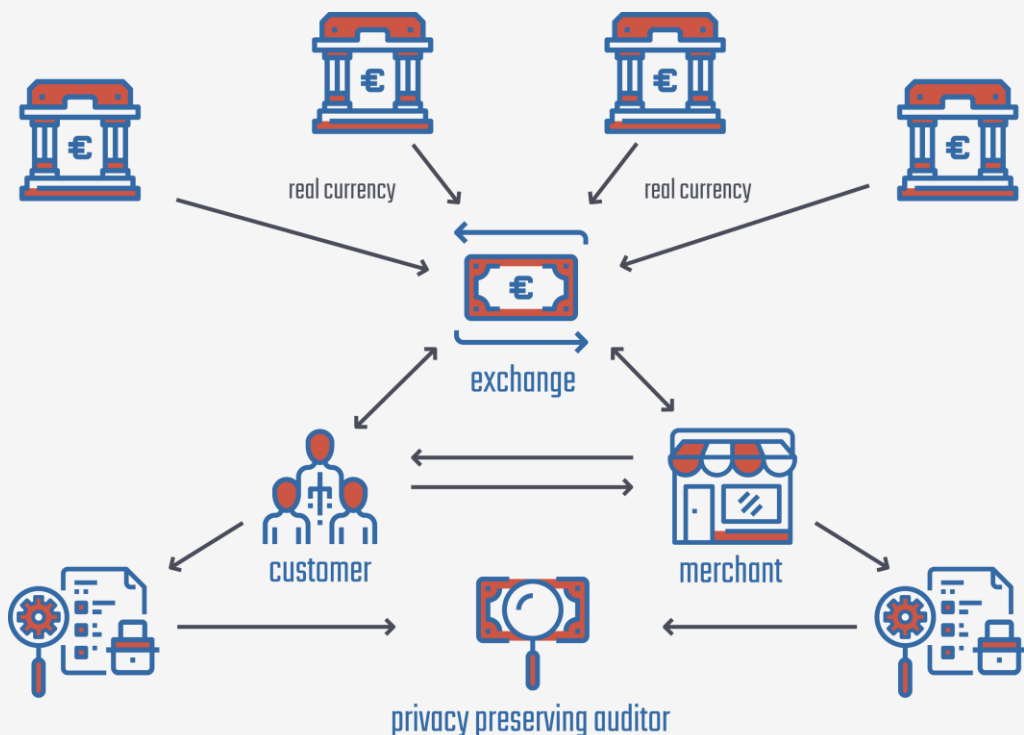
An image of the example running on an early version of the prototype

## USES CASES STATUS

### PRIVACY PRESERVING DIGITAL CURRENCY

#### Overview of Current work

**Atos** is working on the integration of **FE** with Blind signed tokenized eCoins to create a new digital currency that enhances the privacy of customers and provides new methods to regulate their use.



#### Next steps

The first step to carry out the whole pilot requires to implement the basis of a Blind Signature payment with eWallet application, eCurrency issuer and eShop modules. In order to showcase the potential of FE in this demo, a new module will be added to perform audits. Then, the FE encryption layer will be added as the final step.

#### Challenges

Blind signature payment systems are well known due to the anonymity they provide to users, the integration of FE schemes into a blind signature scheme and the management of the corresponding digital keys could provide a way to break this anonymity.

- 1** Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on Falcon | [Design Automation Conference 2019](#)  
*Authors: Angshuman Karmakar, Sujoy Sinha Roy, Ingrid Verbauwhede, Frederik Vercauteren*
- 2** Efficient Function-Hiding Functional Encryption: From Inner-Products to Orthogonality | [CT-RSA 2019](#)  
*Manuel Barbosa, Dario Catalano, Azam Soleimani and Bogdan Warinschi*
- 3** Privacy-Enhanced Machine Learning with Functional Encryption | [ESORICS](#)  
*Authors: Tilen Marc, Miha Stopar, Jan Hartman, Manca Bizjak and Jolanda Modic*
- 4** emmy – Trust-Enhancing Authentication Library | [IFIPTM](#)  
*Authors: Miha Stopar, Manca Bizjak, Jolanda Modic, Jan Hartman, Anže Žitnik, and Tilen Marc*
- 5** Decentralizing Inner-Product Functional Encryption | [Public Key Cryptography \(2\) 2019](#)  
*Authors: Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, Hendrik Waldner*
- 6** Unbounded Inner-Product Functional Encryption with Succinct Keys | [ACNS 2019](#)  
*Authors: Edouard Dufour-Sans and David Pointcheval*
- 7** Obfuscating Simple Functionalities from Knowledge assumptions | [Public Key Cryptography \(2\) 2019](#)  
*Authors: Ward Beullens and Hoeteck Wee*



**DOWNLOAD**  
**FENTEC**  
**LATEST PAPERS**

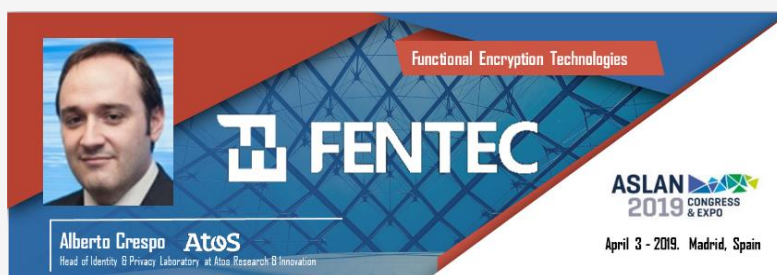


# FUNCTIONAL ENCRYPTION TECHNOLOGIES

## EVENTS

**Paris Technical Meeting:** On April 2nd to 4th 2018, FENTEC Consortium celebrated the 2nd Technical meeting in Paris. All WP discussed, all partners attending. Set up next steps, and several agreed actions

**ASLAN 2019:** On April 3rd our colleague Alberto Crespo delivered a speech on the ASLAN Congress and Expo in Madrid (Spain) under the track "Power of Business Data: Intelligence, analysis and management of the key active on the Digital Era". On his speech he presented FENTEC project and the different use cases that we are working on. If you did not have the chance to attend, visit the following link to see the presentation



**EEA 2019:** On 18th and 19th of June, our colleague Miha Stopar presented The FENTEC Project: Functional Encryption Technologies in the 32nd EEMA Annual Conference in London. He was one of the speakers within the Interactive Session: "Initiatives to Enable Enhanced Privacy and Security".



## FENTEC GOES SOCIAL


During the last 6 months of the project, we have been more active than ever. We generated public content to spread the word about **FENTEC and Functional Encryption**, and it is available for everyone!

On February 6th, our colleague Francisco Gala was interviewed by **COPE Lleida Radio**, a Spanish radio station. During the radio show they talked about Functional Encryption and **how FENTEC is facing the key challenges** within the project. The podcast is published in our website, so if you are a Spanish speaker do not hesitate to visit the link:

[Listen to it!](#)

 @FENTEC\_Project

 FENTEC Project

 Last post!

Apart from that, the project Consortium started the **FENTEC Blog** in 2019 where we share our expertise and knowledge in a comprehensible way for the general public on functional encryption topics.

[Read more!](#)

MORE THAN 300 FOLLOWERS!

@FENTEC\_Project



**FENTEC project** is currently in the middle of its planned duration, so it is time to prepare the first official review meeting that will take place on **4-6th November**.

Before meeting in November, the Consortium organizes a **General Assembly** in **September** hosted by Kudelski. Accordingly, the upcoming work will be focused on the preparation of these meetings. During the third week of September, the **FENTEC Consortium** will meet near Lausanne, Switzerland, to put in common the latest developments and prepare the next review meeting in the presence of the **European Commission**.

In the first review meeting, which will take place in Leuven, Belgium, the **Commission** will evaluate the work performed during the first 18 months in the project, where the three use cases acquire special relevance.

In the meantime, **the FENTEC project advisory board** will meet in Madrid, Spain, at the ATOS' headquarters late in September; this meeting will be an opportunity to collect the experts' comments in order to improve the developments.

Are you interested in  
**FUNCTIONAL**  
**ENCRYPTION?**

Visit [fentec.eu](http://fentec.eu)!



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780108. Any dissemination of results here presented reflects only the consortium view.