D2.6 Exploitation Plan

Document Identification			
Status	Final	**Due Date**	31/12/2019
Version	1.0	**Submission Date**	31/01/2020

Related WP	WP2	**Document Reference**	D2.6
Related Deliverable(s)	D2.7	**Dissemination Level (*)**	PU
Lead Participant	WALLIX	**Lead Author**	Mariem Krichen
Contributors	ATOS, KUD, FUAS	**Reviewers**	Jose Crespo (ATOS) Miha Stopar (XLAB)

Keywords:

SWOT, Market Analysis, Intellectual Property, Exploitation, target market, technology foundation

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.

(*) Dissemination level.-PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	**Partner**
Mariem Krichen	WALLIX
Brecht Wyseur	KUDELSKI
Jose Crespo	ATOS

Document History			
Version	**Date**	**Change editors**	**Changes**
0.01	18/09/2019	Mariem Krichen (WALLIX)	First Draft
0.02	12/12/2019	Jose Crespo (ATOS)	ATOS use case relative sections filled
0.03	06/01/2020	Brecht Wyseur (KUDELSKI)	KUD use case relative sections filled
0.04	07/01/2020	Mariem Krichen (WALLIX)	WALLIX use case relative sections filled
0.05	13/01/2020	Miha Stopar (XLAB)	Document reviewed. Minor comments and typos fixed.
0.06	14/01/2020	José Crespo (ATOS) Francisco Gala (ATOS)	Document reviewed. Minor comments and typos fixed.
0.07	15/01/2020	Mariem Krichen (WALLIX)	Corrections after internal review
0.08	21/01/2020	Mariem Krichen (WALLIX)	Add conclusion section
0.09	28/01/2020	Mariem Krichen (WALLIX)	Add Edinburgh, KUL contribution to academic results section Take into account reviewers' comments
0.10	30/01/2020	Miha Stopar (XLAB)	Final revision. Minor fixes and corrections
0.11	30/01/2020	José Crespo (ATOS)	Final revision. Minor fixes and corrections
1.0	31/01/2020	Diego Esteban (ATOS)	Final version for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Mariem Krichen (WALLIX)	30/01/2020
Technical Manager	Michel Abdala (ENS)	31/01/2020
Quality Manager	Diego Esteban (ATOS)	31/01/2020
Project Coordinator	Francisco Gala (ATOS)	30/01/2020

Table of Contents

List of Figures

List of Tables

List of Acronyms

Abbreviation / acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
APM	Alternative Payment Methods
AWS	Amazon Web Services
CA	Consortium Agreement
CAGR	Compound Annual Growth Rate
CPDP	Privacy Forum, and Computers, Privacy and Data
CLI	Command Line Interface
EC	European Commission
EU	European Union
E2EE	End-to-end encryption
FE	Functional Encryption
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Intellectual Property or Internet Protocol, depending on context
LDM	Local Decision Making
PO	Project Officer
POS	Point of Sale
SME	Small-Medium Enterprise
SWOT	Strength Weakness Opportunities Threats (e.g. market/product analysis technique)
TRL	Technology Readiness Level

Executive Summary

This deliverable provides a strategic foundation to define an appropriate exploitation for the FENTEC project results. The Exploitation Plan identifies the expected outputs of FENTEC, and the methods used or to be used by partners in order to exploit the results. In this document, we have considered three different routes of exploitation.

Firstly, the academic results are published in many scientific conferences in order to attract other researchers and get them involved with the ideas of the project, thus helping to build a community around this project. Through their combined research efforts, the academic partners provide theoretical background and develop state-of-the-art technologies thus contributing to the success of FENTEC.

Secondly, the FENTEC library gives the basics to use cases holders and allow XLAB to get closer to open source community and to offer them consultancy. This library is integrated to the actual prototypes and will be incorporated to their commercial offerings in the future.

Finally, the use cases results are in the heart of FENTEC exploitation plan. Industry partners of the project, WALLIX, ATOS and KUDELSKI, provide real-world use-cases that are inspired from their needs. The exploitation plan of the FENTEC results of industrial partners have been demonstrated via the market and the SWOT Analysis for each of the use-cases, and the exploitation of the results of this project have already placed Europe on the cutting-edge of the deployment of privacy-enhancing solutions based on FE Technology.

1 Introduction

1.1 Purpose of the document

This report aims at presenting the possible routes to exploit research results, gained knowledge, designed software and prototypes, provided by FENTEC project. The goal of exploitation in projects involving both academics and industry like FENTEC is to provide the sustainability of the project results and to keep them alive after the end of the project.

In FENTEC, partners produced three distinctive types of results: Research results and knowledge, Open Source library and Prototypes.

The results of the market study and the SWOT analysis conducted by use cases holders are also presented in this deliverable. Having a market strategy and an action plan are necessary to provide a vision of how prototypes could be brought to market.

The purpose of the document is to present the exploitation plan of FENTEC results until M24. A more detailed study is expected to be conducted for the deliverable D2.7.

1.2 Structure of the document

The document is structured as follows:

- **Section 1:** Introduction
- **Section 2**: Rights and obligations of the members of the Consortium
- **Section 3**: Possible routes of exploitation
- **Section 4**: Market Analysis
- **Section 5**: FENTEC Technology Assessment
- **Section 6**: Conclusion

2 Rights and Obligations of the Members of the Consortium

2.1 Intellectual Property

2.1.1 Rules

The reference documents that describe the way the intellectual property is managed in the project are the Grand Agreement (GA) and the Consortium Agreement. The GA is an agreement between the EC and the FENTEC partners while the CA is an agreement between the partners only. Both documents deal with Foreground (ownership transfer, protection, use and dissemination) and access rights.

2.1.2 Patents

A provisional patent application was filed to protect the IP of Kudelski's IoT use-case in WP7. More information will follow up in future reports.

2.2 Consortium Agreement

2.2.1 Joint ownership

The Consortium Agreement (CA) defines the notion of joint ownership when several partners have jointly generated a Foreground where the amount of respective contribution cannot be clearly estimated. If this situation occurs, the joint owners of the result(s) need to agree on the allocation and terms of exercise of their joint ownership, to ensure compliance with their obligations under the Grant Agreement (Article 26). In addition, each joint owner can grant non-exclusive licenses to other entities unless the joint ownership agreement says otherwise and if the other joint owners are given 45 days advance notice and a fair and reasonable compensation.

Another feasible option gathered in the GA is the possibility to apply another regime than joint ownerships such as transfer of Foreground to a single owner allowing access rights for the other party(ies).

The general strategy of the project and its work plan is to avoid joint IP as much as possible, i.e., whenever possible and whenever it does not hamper the project implementation or introduce additional risks.

The results generated within FENTEC project are collected in the table below, and relevant information to analyze potential joint ownership conflicts is provided for each asset.

N	Result	Owner	IPR of Foreground	Expected TRL
1	Hardware-based API	KU LEUVEN	Open Source	TRL4
2	Software-based API	XLAB	Apache License 2.0	TRL5
3	IoT Use case	KUD	Open Source	TRL4
4	Web Analytics Use Case	WALLIX	Apache License 2.0	TRL4
5	Digital Payments Solution	ATOS	Open Source	TRL4

Table 1 - IPR and expected TRL of FENTEC results

2.2.2 Transfer of Foreground

The transfer of the ownership of a partner's Foreground is described in the CA based on procedures detailed in the Grant Agreement. In this phase of the project no transfer of ownership has been identified.

2.2.3 Access rights

As defined by the GA, the access rights consist of licenses and user rights to Foreground and Background. The Article 31 of the Grant Agreement sets up the access rights according to the type of entity and use of the results.

Access rights for other beneficiaries, for exploiting their own results must be given under fair and reasonable conditions according to Article 25.3 (Article 31.3), but it should be requested up to one year after the end of the project (unless agreed otherwise). Access to the results must also be given to affiliated entities in EU member states if this is needed for those entities to exploit the results generated by beneficiaries to which they are affiliated.

Access to EU institutions must be given on a royalty-free basis, necessary for developing, implementing or monitoring their policies or programs in the area.

Access rights for third parties have not been defined.

2.3 Concrete Licensing Plans between Partners

All the academic partners have agreed to open source the vast majority (if not all) of the prototype software that they developed in the project. That way, the industrial partners and potential third parties can access the project results. If they wish to do so, the industrial partners can also negotiate access rights via other licenses, as described in detail in the CA.

3 Possible routes of exploitation

This section defines the different ways in which FENTEC results may be exploited. We decided to divide the possible routes into three main categories: scientific (academic results), commercial (use cases results) and open source (FENTEC library).

- The scientific category covers academic results representing the basis for FENTEC final products.
- The commercial category covers the use cases results: Web Analytics use case, Digital payment solution use case, IoT use case.
- The open source category covers FENTEC library which offers suitable cryptographic protocols to each use-case need.

3.1 Exploitation Team

FENTEC partners agreed to appoint an exploitation team to deal with the exploitation plan activities.

The Exploitation Team was created to foster and facilitate the innovation process. In order to achieve such mission, one representative per exploitation route and an exploitation manager were selected to facilitate the transfer of FENTEC project results to the market.

The exploitation team consists of:

- An exploitation manager
- A representative from each use case holder
- A representative from library support
- A representative from all academic partners

Mainly, the tasks of this team are to identify the exploitable results, to conduct the market analysis and analyze potential market opportunities.

3.2 Possible routes

3.2.1 Academic results

Academic results are the basis of the FENTEC project. Cryptographic protocols based on Functional Encryption were designed in order to fulfill the requirements of the use cases.

The actions within scientific exploitation include publications, independent research and follow-up projects that adopt parts of the research potential developed through the FENTEC project.

Note that so far academic results have been published in 7 scientific publications in the first year and 12 others in the second year00. In addition to that, academic partners offer seminars, lectures, workshops related to the project. Moreover, the FENTEC academic results indicate future research directions. Indeed, an obvious approach of scientific exploitation is to use FENTEC research as the basis for future publications and research projects. In that sense, academic partners are actively seeking for opportunities that will allow to continue research within scientific threads that have been created during the FENTEC project.

- The ENS team has been continuously extending its research plans regarding FE. The current and future research directions are mainly focusing on improving the efficiency and flexibility of FE schemes with respect to their functionality and security. One of the main directions is to extend FE to a multi-user setting where the data being encrypted is tied to specific labels which are strictly controlled. For better efficiency, ENS is considering solutions in both the random-oracle and standard models and based on different complexity assumptions. ENS is also collaborating with XLAB and KUD to address a challenge regarding the key size of LWE-based constructions.
- UH has been in contact with Huawei Mobile Security Laboratory of Huawei Finland and gave a presentation about FE and UH’s part in FENTEC in their Cyber Security Design and Innovation Workshop on August 29, 2019, in Vieramäki, Finland. UH and KUD are making research on efficient and secure implementation of FE schemes and improving the practical feasibility of FE in those respects.
- The UEDIN team has been working on introducing new security definitions in the area of functional encryption that consider a dishonest encryptor and a dishonest key generator. This is contrary to a dishonest evaluator as in the classical security definition of functional encryption. This project will also cover a Universal Composability analysis to show the meaningfulness of the new introduced definitions. Beside this, the UEDIN team is also working on a black-box extension of private key single input functional encryption into the multi-client setting for a more general class of functions. For this project, also an extension to the decentralized multi-client setting will be considered.
- KUL will leverage the experience acquired throughout the project for further research proposals, potential publications and presentations at conferences and fora, such as the Privacy Forum, and Computers, Privacy and Data protection conference (CPDP).

3.2.2 FENTEC library

XLAB has developed a fully open-sourced library for functional encryption. All code, including cryptographic primitives, cryptographic protocols, and any supporting code, is released in FENTEC GitHub repository.

For each use case, a suitable FE based protocol was designed by academics. XLAB implemented each of these protocols in the language requested by the use case holder. XLAB is also implementing a website where FENTEC libraries and their potential use cases will be presented and visualized. The website will serve also as an online interactive course where cryptography from basics up to the functional encryption schemes will be possible to learn.

Another exploitation path XLAB is targeting is a platform offering privacy-enhanced machine learning. The platform is based on the FENTEC libraries and a paper Privacy-Enhanced Machine Learning with Functional Encryption 0. It aims to enable the application of various machine learning classifiers on the encrypted data and thus enable users to get accurate prediction services while their data remains secret.

Recently there was an increased interest for FENTEC libraries if we observe the number of stars on GitHub. Right now, it is:

https://github.com/xlab-si/emmy 110 stars https://github.com/fentec-project/gofe 52 stars

https://github.com/fentec-project/CiFEr 19 stars

Besides, Free Open Source library provides a significant potential for Consultancy services and allows the project results sustainability while engaging a critical mass of developers and end-users. FENTEC partners or third parties will be free to develop commercial services based on the FENTEC library.

3.2.3 Use cases results

During the project, direct exploitation of the use cases results is limited by the fact that we have only prototypes. The use cases holders aim at turning these protocols into products but productization will probably only be possible after the project ends. The use cases holders can also think of patent applications. Possible exploitation of use cases results is detailed in section 4.

4 Market Analysis

For each of the use-cases of the FENTEC project, we present an analysis of the respective market.

4.1 Internet of Things Market (Kudelski)

The Kudelski Group (SIX: KUD.S) is a world leader in digital security and a provider of end-to-end convergent media solutions, including services and applications requiring access control and rights management to secure the revenue in digital television, internet, mobile and interactive applications. Next to its tradition digital television security services, the Kudelski Group is also providing product and services for cyber security and IoT.

With its IoT division, the Kudelski Group has developed an IoT security platform, which enables IoT device manufacturers and solution providers to develop secure end-to-end solutions. The focus of the technology is to secure customers' business models by securing its operations and providing full lifecycle services – from design and secure operation to monitoring and response.

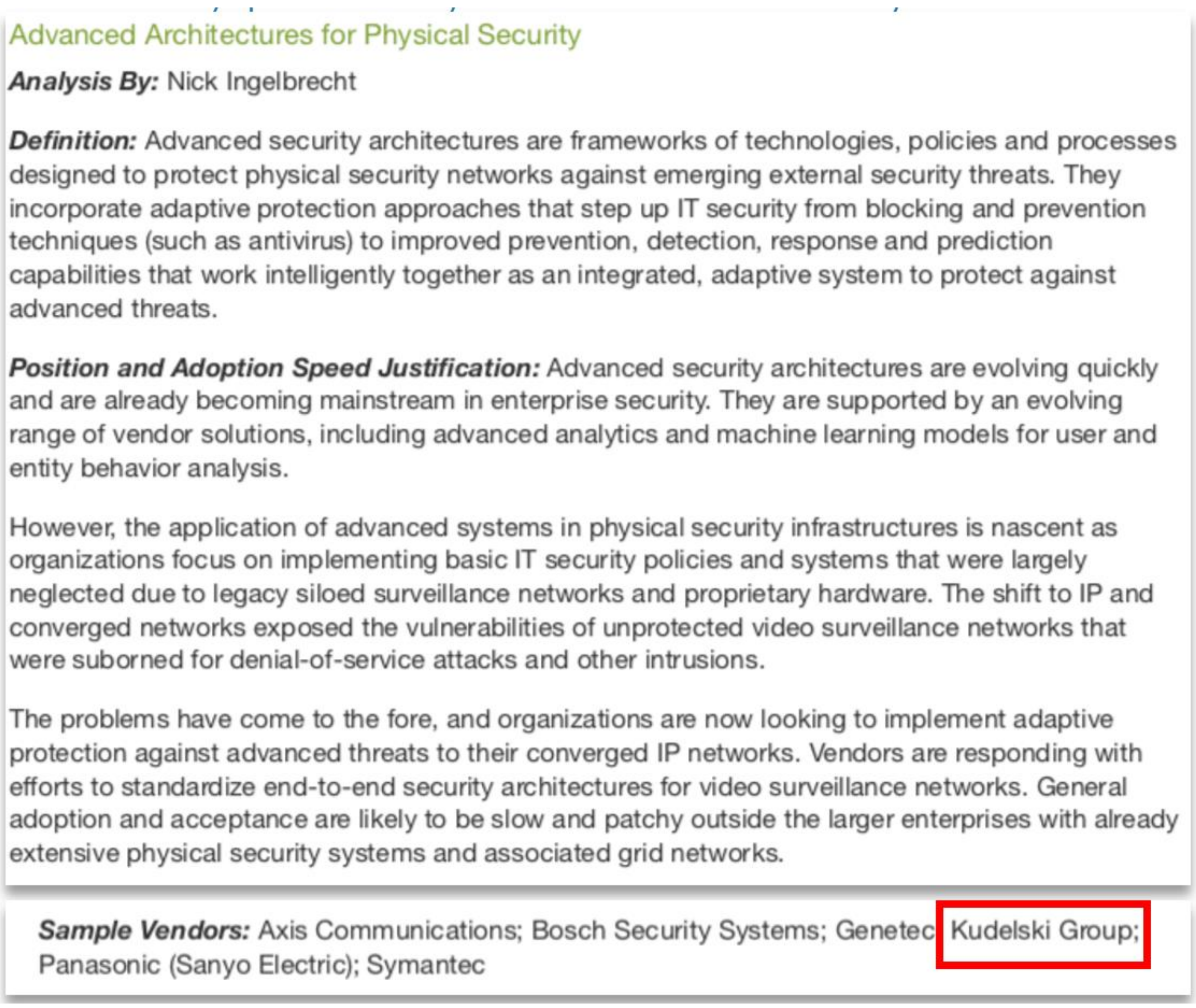
As part of the solutions, Kudelski is integrating technology into Edge devices. These are IoT gateways which make the link between IoT devices (such as cameras, sensors, actuators, etc.) and cloud platforms (such as Azure, AWS IoT, or on-premise platforms). Edge gateways are introduced into an IoT ecosystem for many different reasons

- To provide connectivity between IoT devices and cloud services. E.g., connecting sensors locally to an Edge device, and then be able to push collected data to the cloud.
- To improve operations: since Edge devices are closer located to the actual IoT operations, it can provide lower latency services or keep operations running even when connection to cloud platforms is (temporary) lost.
- For Local Decision Making (LDM). The traditional IoT model is to aggregate data from devices and compute on their data in the cloud. This model is changing however, where compute is taken "out" of the cloud onto devices that are closer to 'Things'. This is often referred to as 'Fog Computing or Intelligent Edge.
- GDPR, data sensitivity and data ownership. Enabling compute on Edge devices rather than cloud is often preferred to comply with GDPR or address challenges with respect to data sensitivity and data ownership. By enabling compute close to things, one can avoid to provide sensitive data to 3rd party cloud systems where this can risk exposure.

4.1.1 Smart Camera Market

Together with SmarDTV, the Kudelski Group has developed a secured video surveillance solution, which allows to update legacy cameras with a "bump-in-the-wire" approach. This solution entails an Edge device that can be installed in legacy smart camera solutions to secure those cameras against cyber-attacks and to enable value add services such as protecting the video stream or enable local decision making. This solution has been presented at CES 2018 and is using the Kudelski secured IoT platform and showing live video content encryption out of an existing retail camera 0.

For this solution, the Kudelski Group is recognized by Gartner, as for example mentioned in “Best Practices for Procurement for Video Surveillance, Analytics and Response Systems in Physical Security”, published on April 17, 2018. “Gartner's Adaptive Security Architecture research covers security-aware solution design, artificial intelligence (AI)-enabled user and entity behavior analytics, and methods to secure endpoints (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"). Companies, including Kudelski Group/Nagravision, are building cross-industry standards and solutions for end-to-end secure surveillance architectures, although it may take many months before those efforts come to fruition.”



Advanced Architectures for Physical Security

Analysis By: Nick Ingelbrecht

Definition: Advanced security architectures are frameworks of technologies, policies and processes designed to protect physical security networks against emerging external security threats. They incorporate adaptive protection approaches that step up IT security from blocking and prevention techniques (such as antivirus) to improved prevention, detection, response and prediction capabilities that work intelligently together as an integrated, adaptive system to protect against advanced threats.

Position and Adoption Speed Justification: Advanced security architectures are evolving quickly and are already becoming mainstream in enterprise security. They are supported by an evolving range of vendor solutions, including advanced analytics and machine learning models for user and entity behavior analysis.

However, the application of advanced systems in physical security infrastructures is nascent as organizations focus on implementing basic IT security policies and systems that were largely neglected due to legacy siloed surveillance networks and proprietary hardware. The shift to IP and converged networks exposed the vulnerabilities of unprotected video surveillance networks that were suborned for denial-of-service attacks and other intrusions.

The problems have come to the fore, and organizations are now looking to implement adaptive protection against advanced threats to their converged IP networks. Vendors are responding with efforts to standardize end-to-end security architectures for video surveillance networks. General adoption and acceptance are likely to be slow and patchy outside the larger enterprises with already extensive physical security systems and associated grid networks.

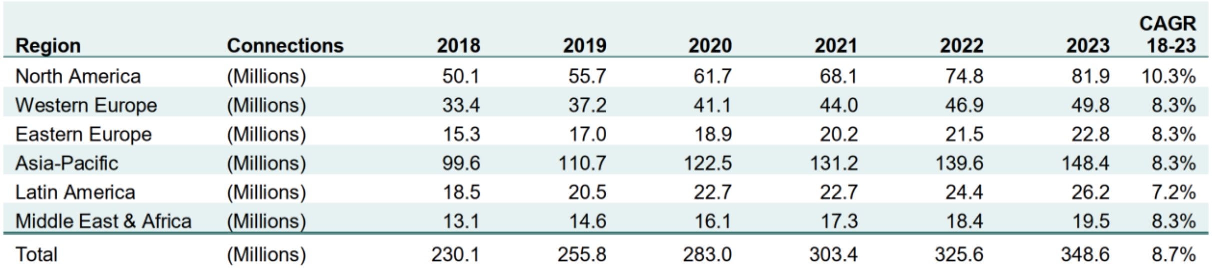
Sample Vendors: Axis Communications; Bosch Security Systems; Genetec Kudelski Group; Panasonic (Sanyo Electric); Symantec

Figure 1 - Excerpt from Gartner's Hype Cycle for Physical Security, 2018. Recognizing Kudelski Group as a vendor in Smart Camera security.

The Kudelski Group is targeting the connected enterprise video surveillance market. Key trends as recognized by ABI research in November 19, 2018 include:

- The number of enterprise video surveillance camera connections will grow from 230.1 million in 2018 to 348.6 million in 2023 at a Compound Annual Growth Rate (CAGR) of 8.7%.
- Overall, enterprise video surveillance value-added services revenue is estimated to grow from US$10.3 billion in 2018 to US$12.6 billion by 2023.

- The Asia-Pacific region will have the greatest share of non-consumer video surveillance camera connections and corresponding revenue over the duration of the forecast period, buoyed by the impact of China's growing surveillance state.
- Privacy laws by country will greatly influence the level to which certain video analytics solutions are implemented with facial recognition features more likely to be used in countries with less restrictive privacy laws, such as China.
- The United States' 2019 National Defense Authorization Act banning the use of Chinese state-owned video surveillance will have an almost immediate impact on the U.S. market by creating a sizable market void that U.S.-based solution providers will have the opportunity to fill.
- The switch from analog to Internet Protocol (IP) cameras is in full swing, but while the majority of deployed video surveillance cameras will use fixed-line IP connectivity, providers should still offer support for legacy systems in the form of encoder, converter, or other integration services in order to fully address the market and guide the laggards' digital transformation.



Region	Connections	2018	2019	2020	2021	2022	2023	CAGR 18-23
North America	(Millions)	50.1	55.7	61.7	68.1	74.8	81.9	10.3%
Western Europe	(Millions)	33.4	37.2	41.1	44.0	46.9	49.8	8.3%
Eastern Europe	(Millions)	15.3	17.0	18.9	20.2	21.5	22.8	8.3%
Asia-Pacific	(Millions)	99.6	110.7	122.5	131.2	139.6	148.4	8.3%
Latin America	(Millions)	18.5	20.5	22.7	22.7	24.4	26.2	7.2%
Middle East & Africa	(Millions)	13.1	14.6	16.1	17.3	18.4	19.5	8.3%
Total	(Millions)	230.1	255.8	283.0	303.4	325.6	348.6	8.7%

Figure 2 - Non-Consumer Video Surveillance Camera Connections by Region. World Markets. Source: ABI Research

Key market verticals for such solution include

- Government applications and critical infrastructure, including airports, bridges, highways, ports, water/nuclear power facilities, utilities complexes, and other public venues, such as sports arenas
- Defense department applications, such as convoy video surveillance and perimeter surveillance at military bases,
- Municipal government organizations, such as police departments and metro transit authorities
- Finance and banking used primarily for theft avoidance
- Retail applications to reduce shrinkage and for behavioral analysis
- Casinos to identify card counters and other non-desirable guests
- Education applications, such as asset protection and access control
- Transportation applications, such as traffic monitoring
- Utilities applications, such as theft detection and creating a virtual perimeter

4.1.2 Smart Camera and FENTEC

As a cyber security company, the Kudelski Group is investing in security technology to enable secured smart camera solutions. It considers its active participation in the FENTEC project as a technology enabler, adding value to its product solutions.

As a security provider, the Group develops end-to-end security solutions, where data is encrypted from the point of origin to where it needs to be consumed. FENTEC technology allows to process the process/consume data without having to decrypt that data, which enables powerful security guarantees.

Within the context of the FENTEC project, Kudelski is applying the FENTEC technology to a use-case for privacy-preserving movement detection. Such use-case is in particular interesting for building security use-cases (Smart Buildings and Smart Cities) and in Critical Infrastructure. The commercial exploitation of these results is supported by partnerships that have been built and active participation of Kudelski Group in strategic alliances and industry bodies. For example,

- Kudelski has a partnership agreement with Securitas AG. A Swiss company founded in Berne, Switzerland, in 1907. Today Securitas AG has 15,000 employees worldwide that offer professional security services such as physical protection and alarm systems.
- Kudelski is developing security solutions for anomaly detection of Critical Infrastructure with undisclosed large Distribution System Operators – in Europe and Japan principally. The main focus is anomaly detection for Electrical Substations.
- Kudelski is an active member of Industry Bodies where Smart Camera security and the FENTEC use-case is actively discussed. In particular in the Electrical Energy market where Kudelski is a member of the European Energy ISAC, World Economic Forum initiative on Cyber Resilience for the Electrical Energy market, and the International Energy Agency.

4.2 Web Analytics Use Case

4.2.1 WALLIX Target Market

The era of the IoT revolution and “on Premise” services migration into the Cloud caused the invasion of individuals privacy. Our personal data turned into a booming global market fuel: Data Monetization.

Often described as the 21st-century oil, data is a key resource that can be expensive depending on its interest levels. The power of data and its possible exploitation abuses could vary from advertising targeting to strategic reversal of an election campaign. Thus, data analyst and services providers collaborate so that each piece of data is scrutinized, analyzed then properly exploited before selling it to interested companies.

Furthermore, this treasure hunt also becomes the hackers' main target by multiplying data servers’ attacks. No one is spared. SMEs and industry giants have experienced the damage of data leakage: employees privacy invasion, loss of credibility from the customers' point of view, judicial liquidation.

In this context, where technological developments often go hand in hand with trust crisis, Europe has set up a unique legal framework, the so-called GDPR (the General Data Protection Regulation), aimed at regulating data economy. Since the entry into force of the GDPR, the concept of privacy by design which is at the heart of the regulation is gaining ground.

The technology of End-to-end encryption (E2EE) embraces this concept, thus attracting cybersecurity editors' interest. Indeed, many software enterprises are adopting encryption solutions since the enforcement of the GDPR law to ensure compliance and to improve data protection.

The risk to data privacy coupled with GDPR compliance obligation is a powerful driver for cybersecurity market expansion. This context enabled the activity scope extension of cybersecurity actors and particularly data and content protection actors. Wallix seized this market growth opportunity to extend its activity from access protection to data protection.

Since Data protection is vital, E2EE enables companies to strengthen the security of their applications in order to avoid data leakage that could be harmful to the employer's image. Indeed, integrating this technology into applications will offer a high level of security to end-users without any change of their user experience while ensuring confidentiality of personal data during transport as well as storage.

In that sense, Wallix plans to launch DataPeps a new E2EE encryption platform for data protection. This event is planned for Q3 of 2020. DataPeps is an "as a service" end-to-end encryption solution that developers can easily and seamlessly integrate in all their applications and infrastructures. DataPeps not only protects data from cyber-attacks, it also ensures that applications comply with the future European General Data Protection Regulation, the GDPR. Down the line, DataPeps will enable users to widen the scope of encryption and protect data in the different forms in which it is used (file sharing, e-mails, social networks and online platforms, connected objects and smart home devices).

However, E2EE shows defects and is facing a functional and psychological barrier: without decryption, any legitimate encrypted data exploitation is hopeless. Functional encryption provides an answer to this problem by proving that it is possible to store data, on Cloud or "on Premise", in an encrypted form and to exploit some for legitimate purposes without decryption process. In fact, Functional Encryption (FE) seems appropriate to ensure statistical analytics on collected encrypted data without revealing them given their personal or strategic nature.

Thanks to FENTEC use case, Wallix wants to provide high added value feature: Statistical analysis on encrypted data to DataPeps in order to reinforce its position in the .

According to a report published by the Grand View Research, the is likely to reach USD 8.74 billion by 2025, progressing at a CAGR of 16.8% during the forecast period. The context described above are expected to fuel product demand over the next few years. The adoption of encryption solutions like E2EE and FE based solutions is on a rise to prevent any incidence of data loss, theft, or leak, whether intentional and to maintain customer loyalty and protecting enterprises' brand reputation. Thanks to encryption solution, User data is protected during transfer and storage and, even if breaches are successful, data is not visible to attackers.

4.2.2 How the use case fits the market?

The use case fits in the market since WALLIX will launch in 2020 DataPeps, a platform for End-to-end encryption (E2EE). Our Web Analytics use case will be a high-added value feature for DataPeps. This feature is meant to reinforce the position of WALLIX in Encryption Software Market since its French competitors (Virgile security and Tanker) do not propose this kind of features.

The FENTEC use case will allow WALLIX to stand apart from competitors and thus to get better position in its target market.

4.2.3 Expected exploitation size

- The size is not yet defined since DataPeps is not yet commercialized.
- This functionality will be proposed to DataPeps clients
  - **Option 1:** For free for all DataPeps clients
  - **Option 2:** As an additional option: a paying option for DataPeps
  - **Option 3:** For free only for premium clients

4.3 Digital Payment Solutions Market (Atos)

4.3.1 Target Market

The Digital Payments Market includes all the payments that are made over the internet as well as mobile payments at point-of-sale (POS) via smartphone applications. Business-to-business payments, bank transfers and transactions where mobile card readers are used are not part of the Digital Payments market. Consumer digital payments are growing rapidly: according to McKinsey[1] the global digital commerce volume exceeded USD 3 trillion in 2017 and will more than double by 2022. Mobile commerce is the most dominant factor in this trend, accounting for 48% of digital commerce sales.

While the online payment experiences have improved over the last years, alternative payment methods (APMs) have gained popularity. The amount of in-store transactions varies significantly by country and region: in countries with NFC infrastructure, tap-and-pay will foster growth; in emerging markets, the introduction of new payments solutions will influence how people pay. In the US, in-person use of digital wallets will increase at a 45 % CAGR to reach nearly USD 400 billion in annual flows for 2022. The global eWallet market is expected to grow at a CAGR of 15% and estimated to reach market size of approximately USD 2.100 billion by the end of forecast period 2017-2023.

4.3.2 How the use case fits in the market?

The digital-based currency use case provides a one-to-one counterpart to physical money, removing the privacy issues but allowing taxability and auditability by governments. The overall solution is more complex that traditional eWallets in terms of technical development, thus it offers higher added value to several stakeholders: end users don’t expose their private information and merchants would have a more cost-effective tool enabling micropayments. Even though the solution is different, it could fit in the eWallet market due to the fact that it offers an efficient alternative for digital wallets.

Segmentation of the solution by mode of payment:

- Point of sale: Mobile contactless payment
- Online sale: Digital wallet, digital currency

According to Capgemini’s World Payment Report, non-cash transactions conducted through e-wallets peaked up on 41.8 USD billion globally. About 71% of this amount was conducted via payment apps and e-wallets offered by big companies. The proliferation of this payment method has been intensified

[1] https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Global%20payments%20Expansive%20growth%20targeted%20opportunities/Global-payments-map-2018.ashx

by the penetration of the smartphones, the change in consumer behavior and regulation. From the end-user perspective, the main drivers for this proliferation are frictionless payments (related with customer experience), security and potential added value that customers get from using the service.

Juniper Research[2] report on digital wallets show how by the end of 2019 there will be 2.1 billion eWallet users worldwide making transactions. Furthermore, around two thirds of the eWallet users are located on the Asia-Pacific geographic area. In the European Union the most advanced country in terms of eWallet adoption is Norway, with 42% of smartphone users making transactions with eWallets.

Innovation in payment methods in different verticals

The new payment solutions offer many application possibilities, but their use and potential added value is different in each vertical. The Payment Methods Report 2019[3] analyzes the impact of the payment methods innovation on three key verticals: retail, travel and gaming industries.

The environment of the retail industry is changing rapidly due the proliferation of new platforms, new providers and new payment tools. Most of the challenges that retailers face today are related with the convenience of the customer journey, so the biggest technological developments aim at speeding up the purchasing process and make it quicker and secure. There is a wide range of solutions, from proprietary banking eWallets and services such as PayPal that are widely accepted by users. Merchants want to offer the maximum number of payment alternatives, so a lot of them have also included cryptocurrencies as payment options (Expedia, Cheap Air).

The payment methods on the travel vertical are highly fragmented, especially on the airlines market. The main challenge for the travel industry companies is to identify which innovations have a higher potential to meet the expectation of the digitalized consumers.

The gaming sector has become an interesting vertical when it comes to payment methods innovations. According to the Newzoo and ACI Worldwide study, 95% of the German, UK and US mobile gaming users choose PayPal as the best payment method. Furthermore, this study also reflects that 75% of the players spend money on in-game purchases. Therefore, we can observe that the gaming industry is likely to become 100% cashless.

Besides global brands such as Apple Pay, Google Pay or Samsung, there is a wide range of European and local eWallet initiatives: Payconiq (Germany, Belgium, the Netherlands), Payback (Germany), Paylib and Lyf Pay (France), Pingit (the UK), Vipps (Norway), Swish (Sewden), MobilePay (Denmark, Finland), and OK (Netherlands). The main sustainability and business routes for these eWallets are developed through the generation of partnerships with retail chains, offering extra value for their clients.

4.3.3 Expected Exploitation Size

The exploitation size cannot be analyzed at the moment due to the fact that the solution needs further development to measure the potential perceived value of users and customers.

The solution has been considered relevant to potentially generate new business in Atos, involving the Innovation Hub team to maximize the impact of the use case. The Innovation hub will evaluate the

[2] Digital Wallets, Juniper Research – Windsor Holden 2019

[3] Payment Methods Report 2019, Innovations in the Way We Pay – Ecommerce Foundation

market feasibility of the solution and will act as a bridge between the Research department and the existing business units of the firm. A minimum viable product should be developed in order to evaluate whether the solution meets potential customer’s needs or not.

5 FENTEC Technology Assessment

5.1.1 SWOT Analysis

In this section, we perform a SWOT analysis of all the technology developed in the FENTEC project, as well as a technology readiness level assessment. The analysis considers all tools and technology as foreseen at the end of the project.

SWOT stands for Strengths, Weaknesses, Opportunities, and Threads. As shown, the former two relate to properties that have internal origins, while the latter two relate to properties that have external origins.

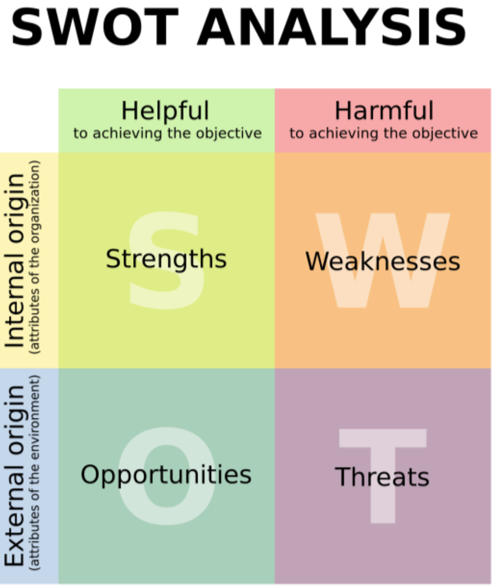

SWOT ANALYSIS
Helpful
to achieving the objective
Harmful
to achieving the objective
Internal origin
(attributes of the organization)
External origin
(attributes of the environment)
S
Strengths
W
Weaknesses
O
Opportunities
T
Threats

Figure 3: SWOT Analysis representation

5.1.2 SWOT analysis justification

The SWOT analysis is appropriate for business planning process and gives a summary to enable decision making. It is flexible, comes at little cost and it does not require a lot a time.

Still, it has limitations; for example, all properties are put at the same level without any way to set priorities. This analysis lacks classification that would help to set a hierarchy among all the properties described. As a consequence, some parasite properties may prevent to give a clear view on the major aspects to be considered for the business.

There are no guidelines to identify elements and because it is a subjective analysis, it falls in psychological traps. Weaknesses are easier to determine then some care must be taken to compensate this tendency to obtain a balanced result. Still about the missing guidance directives, Opportunities could be switched to Threads and vice-versa according the personality/experience/intuitiveness of the evaluator.

The split proposed in four categories is not appropriate for uncertain property that may fall in two categories like Strength and Weakness; with respect to these two-sided factors, the SWOT is too rough.

The proposition is to use this SWOT analysis at this early stage on the path of a future industrialization of FENTEC. More in-depth research and detailed analysis would help to secure the evaluations but still, keeping in mind it is only to be used at the first evaluation of the business planning process the outputs seem relevant enough to be used for the project.

5.1.3 Readiness level evaluation

For the maturity analysis, we will rely on the EC H2020 definition of technology readiness levels (see http://en.wikipedia.org/wiki/Technology_readiness_level - European_Commission_definition):

Technology Readiness Level	**Description**
TRL 1.	basic principles observed
TRL 2.	technology concept formulated
TRL 3.	experimental proof of concept
TRL 4.	technology validated in lab
TRL 5.	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6.	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7.	system prototype demonstration in operational environment
TRL 8.	system complete and qualified
TRL 9.	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

5.2 FENTEC Use-Cases

5.2.1 Internet of Things use-case (Kudelski)

- Strengths
    - Meaningful use-case with validated exploitation opportunity in the market of Smart Building and Infrastructure Video Surveillance.
    - Can be deployed on existing Edge gateways
- Weaknesses
    - Considerable processing power needed

  - The use-case as implemented in FENTEC only applies to motion detection, while other parameters in video streams (and in particular AI/ML processing) can be of increasing interest.
- Opportunities
  - Many optimizations to reduce processing power can be applied. Such as analysis of a reduced set of frames.
- Threats
  - Motion detection can be integrated into cameras themselves rather than on Edge devices. This however requires more costly cameras and does not apply to legacy systems. Today, this is not a threat due to price points, but this situation may evolve.
  - Alternative solutions, with isolated security hardware that does secure processing and access control to encrypted video streams could take market share.

5.2.2 Web Analytics use case

- Strengths
  - The web Analytics use case is a use case that meets the needs of web application users in terms of confidentiality
  - A good GDPR (Global Data Protection Regulation) compliance and Privacy By Design concept insurance
  - A continued pursuit of the Wallix strategy. After the success of Wallix Bastion for access securing, DataPeps platform for securing Data will complete Wallix offer. Web Analytics use case is meant to be a future feature of DataPeps.
  - Web Analytics use case offers a high added value to DataPeps and helps to set it apart from competitors.
- Weaknesses
  - Exploitation of web analytics use case is closely linked to DataPeps exploitation
- Opportunities
  - GDPR: Since 2018, May 25th European companies are required to comply with the rules of GDPR. Encryption is an excellent tool for compliance.
  - Cloud Act: Encryption is today considered as the only valuable solution to fight against the Cloud Act if your hosting data provider is American.
  - European companies' interest on Privacy By Design
- Threats
  - Very competitive market and some competitors have started deploying their solution
  - Differential Privacy is a non-cryptographic tool that allows secure analytics

5.2.3 Digital Payment Solutions Market (Atos)

- Strengths
  - S1: High level of privacy and security: The use case demonstrates several benefits regarding privacy and security, one of the main concerns that end-users have when making transactions with new payment methods.
- Weaknesses
  - W1: Low TRL

- Opportunities
    - O1: Consumer’s perception of security and privacy. The new payment technologies drive fears around identity theft and privacy issues that have a chilling effect when it comes to adopting mobile ecommerce solutions. The adoption of new payment solutions is being slowed down due to end user concerns on regard of privacy and security. This reality is considered as an opportunity due to the fact that one of the main characteristics of the digital payment use case is the privacy-preserving policy, that could be an important driver for the adoption of the solution.
    - O2: Digital Payments Solutions market growth

- Threats
    - T1: Highly competitive market
    - T2: Big competitors leading the market with relatively high barriers of entrance

5.3 Technology Foundations

5.3.1 AWLESS

AWLESS is an open-source command line interface (CLI) which allows the creation, update and deletion of resources on Amazon Web Services (AWS). The AWS service is a complex system allowing deployment of cloud-based instances of computing platforms on a subscription basis. A large variety of instances and instance sizes as well as geographical locations and routing options are provided. There is also a large number of software options for these instances including databases, Web servers, different kinds of storage devices, mobile features, automated load-balancing, analytics, access policy control and many others.

This creates a problem for system managers who have to implement and maintain this huge network of hardware and software. While all of this can be managed by Amazon’s labyrinthine online user interface it cannot be easily automated.

There is also an extensive API allowing remote control of AWS configurations, but this is also very complex. To simplify the automation and management of AWS accounts therefore, one popular option is to use a CLI.

There are actually several CLI interfaces available, including one from Amazon itself. AWLESS has several features which make the process easier. Firstly, AWLESS downloads the configuration data into a local graph structure enabling fast local analysis of the current AWS state. Secondly, it is equipped with a fast templating language which allows the rapid design and construction of AWS infrastructures. This allows AWLESS to provide very intelligent lists of options for systems maintainers during the development process. Access patterns to AWS services could be used predictively to provide better suggestions and to even allow optimization of the services deployed on AWS. Hence, we think that analysis of access pattern data could lead to useful information for improving the development process and for optimizing the use of these services.

Note that there are actually two possible ways the FE technology could be used. Firstly, we could incorporate our methods into AWLESS itself in order to analyze the developer’s most used access patterns and secondly, we could incorporate our FE methods into the instances deployed in order to provide the developer with information about the users of their systems.

5.3.2 FENTEC Library

FENTEC project developed two open-source libraries for functional encryption – GoFE [4] and CiFEr [5]. Functional encryption enables computation on encrypted data and presents a viable alternative to homomorphic encryption. Functional encryption can be used for example for creating a heatmap from location data of users in a way that the data of each individual is anonymous and encrypted [6]. Furthermore, it can be used to develop private predictive analysis services, for example for computation of the risk of general cardiovascular disease solely on the base of encrypted data [7]. Also, it enables the application of machine learning algorithms on encrypted data [8].

The three demonstrators can serve potential adopters of GoFE and CiFEr to see the power of functional encryption and to become acquainted with GoFE and CiFEr API. The advantages (and some disadvantages) of functional encryption compared to homomorphic encryption can be found in [1].

6 Conclusions

During the last period of the FENTEC Project, exploitation activities have been mainly focused on three aspects:

- Analysis and definition FENTEC exploitable results
- Diagnosis of the market potential of FENTEC assets
- Identification of the initial partners’ exploitation interest and intentions

It is difficult to produce an exploitation plan of a collaborative project before its end. Indeed, the strategy of a partner could vary in the middle of the project depending on the results. This deliverable is a general overview of the possible routes to exploitation of academic partners, FENTEC library designer and use cases holders.

In the next deliverable D2.7, each partner will detail its Project results exploitation, specify the expected future project exploitation when it ends and indicate the strategy and the motivation. This document is thus intended to be much more detailed and consistent than the D2.6

References

[1] Tilen Marc, Miha Stopar, Jan Hartman, Manca Bizjak, Jolanda Modic, Privacy-Enhanced Machine Learning with Functional Encryption, In Proceedings of the ESORICS'19, the 24th European Symposium on Research in Computer Security, 2019.

[2] FENTEC D2.4: Annual Dissemination Report & Material Y2 – Page 9 and 10

[3] FENTEC D2.3: Annual Dissemination Report & Material Y1 – Page 9 and 10

[4] https://github.com/fentec-project/gofe

[5] https://github.com/fentec-project/CiFEr

[6] https://github.com/fentec-project/FE-anonymous-heatmap

[7] https://github.com/fentec-project/privacy-friendly-analyses

[8] https://github.com/fentec-project/neural-network-on-encrypted-data