D2.11 Preliminary Standardization Report

Document Identification			
Status	FINAL	**Due Date**	30/06/2019
Version	2.0	**Submission Date**	28/06/2019

Related WP	WP2	**Document Reference**	D2.11
Related Deliverable(s)	D2.1, D2.12	**Dissemination Level (*)**	PU
Lead Participant	KU Leuven	**Lead Author**	Svetla Nikova
Contributors	Svetla Nikova (KU Leuven), Kimmo Järvinen (UH)	**Reviewers**	Kimmo Järvinen (UH)
			Francisco Gala (ATOS)

Keywords:
Standardization, Functional Encryption

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
Svetla Nikova	KU Leuven
Kimmo Järvinen	UH

Document History			
Version	Date	Change editors	Changes
0.1	01/06/2019	Svetla Nikova (KU Leuven)	ToC
0.2	27/06/2019	Svetla Nikova (KU Leuven)	Content added
0.3	27/06/2019	Kimmo Järvinen (Partner)	Internal review
1.0	27/06/2019	Svetla Nikova (KU Leuven)	Final version for submitting

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Svetla Nikova (KU Leuven)	27/06/2019
Technical Manager	Michel Abdalla (ENS)	27/06/2019
Quality Manager	Diego Esteban (ATOS)	28/06/2019
Project Coordinator	Francisco Gala (ATOS)	28/06/2019

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
ABE	Attributed Based Encryption schemes
AES	Advanced Encryption Standard
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ECC	Elliptic Curve Cryptography
ENISA	European Union Agency for Network and Information Security
ESO	European Standards Organization
ETSI	European Telecommunications Standards Institute
FE	Functional Encryption
IBE	Identity Based Encryption
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
RSA	Rivest-Shamir-Adleman cryptosystem
SHA	Secure Hash Algorithm
SRM	Standard Reference Material
WG	Working Group

Executive Summary

This deliverable, FENTEC's D2.11, is the first of two standardization reports that are planned within the lifetime of this project. Standardization activities are, together with dissemination, communication and exploitation activities, the backbone of FENTEC's work package 2, whose main focus is to promote and achieve high impact and visibility for the research and innovation outcomes resulting from this project. Standardization efforts are essential to ensure that existing standards are used by the project whenever possible as well as to contribute to current standardization efforts and promote new standards. In this first report we provide a description of the different activities related to standardization that we have carried out so far in the first half of this project.

Our standardization activities can be classified along two main lines. Firstly, we have pursued the adoption of existing standards, namely, we have mapped out existing standards relevant to the problems and envisioned solutions being considered in this project.

Secondly, we have sought to lay out a plan to contribute to current drafts and potential new standards. We have engaged with several standardization organizations in order to explore different collaboration possibilities. The most notable among these is ETSI, which is an ESO. ETSI is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. We have established a liaison with ETSI and contribute to its activities via the partners from FENTEC, who are members of ETSI, namely, ENS and Nagravision. The liaison allows us to provide input and actively contribute to standards in the field of cryptography.

We conclude with an outlook of the standardization activities we plan to focus our efforts on during the second half of this project, namely, keep exploring standards relevant to our project as well as contributing to ETSI standards currently under development through our liaison. We are also in application procedure for a liaison with ISO, which we hope to finalize soon.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to report on the standardization activities carried out by FENTEC in the first half of its lifetime. This is the first of two reports on standardization planned to be delivered during the whole duration of the project. This first report focuses on the mapping out of existing standards, both those already published and accepted by the community, and those that only recently have started to be drafted out. Our first goal is to provide an overview of those standards that are relevant to the project and those that could potentially be.

The second goal of this report is to expose gaps in the standardization, namely, to report on those research areas that FENTEC is involved in where no relevant standards exist or have been published or initiated so far. We couple this with an analysis of how realistic or feasible it is to expect standardization activities in these non-standardized domains.

The third goal of this document is to inform the reader about our initial contacts with standardization bodies and other working groups. From the type of standardization activities, they are carrying out at the moment, together with their methods and requirements to the standardization process, we provide a first outline of the future possibilities we have so far considered promising for the research outcomes stemming from FENTEC.

This will be further explored during the second half of the project, when the research outcomes are mature and can be properly explained to and understood by the rest of the research community and standardization bodies.

1.2 Structure of the document

This document is structured as follows. In Section 2 we motivate the need for standardization and introduce and describe the types of activities we have carried out so far in the project. In Section 3 we describe the standardization bodies. In Section 4 we discuss the adoption of existing standards, while in Section 5 we report on our contacts with standardization bodies and the standards under development or even future standards that we have considered contributing to. Lastly, in Section 6 we conclude by providing a short discussion on what has been done in terms of standardization so far and an outlook of what the focus of our activities will be in the remaining half of the project.

2 About Standardization

Standardization is increasingly viewed as an essential activity to secure a robust foundation for research and innovation efforts. Standardization efforts bring several advantages to the research and innovation community. They prevent the emergence of compatibility and interoperability problems by bringing teams working on similar problems closer, which in turn allows different teams to build on each other's efforts and test each other's advances, overall resulting in better quality control and thorough experimentation. The importance of standardization has been recognized by the European authorities as key for innovation and sustainable economic growth and has therefore become an important component of current and future research and innovation actions.
Still, it is important to note that standardization can also pose certain problems. Too early attempts to standardize a technology, which is still in its infancy, may stiffen and wither innovation, preventing better solutions from arising due to the constraints imposed by a premature standard. This is particularly important for cryptographic primitives where enough time needs to pass to allow the community to study the security of a proposal in order to build up confidence that the proposal is indeed secure. Also, pushing standards through without enough consensus can result in multiple standards that must compete with each other, thereby defeating one of the very purposes of the standardization process, harmonization.
In FENTEC, this is an especially sensitive issue. Our research spans a research area still in its infancy, therefore, making the task of producing robust and reliable standards a true challenge. Still, contributing to standardization involves much more than producing new standards. Adopting previous standards and understanding and influencing standards currently underway is just as important. In FENTEC, we aim to explore all avenues and thus our standardization efforts are being carried out on various fronts.

2.1 The Approach of FENTEC to Standardization

FENTEC standardization activities can be classified according to three main types of actions. We devote subsequent chapters of this report to detail what advances have been achieved so far with respect to each of these activities.

- **Adoption and revision of existing standards**. First, we are adopting, where possible, international standards that are relevant to our project. By doing so, we support previous innovation efforts and contribute to the strengthening of existing standards. Moreover, adopting existing standards involves a critical revision that helps finding gaps and shortcomings. This analysis is key to revise and ultimately improves existing standards.
- **Contributing to current standardization efforts**. Second, we are trying to engage, to the best of our ability, with standardization bodies and their respective working groups in an attempt to contribute to their standardization efforts. Rather than launching or proposing standards ourselves, our goal is to join in already existing standardization initiatives, providing input and participating in the discussions to assist to the elaboration of better standards. Our input can be valuable in that we are developing new technologies and solutions, both at a fundamental research and commercial innovation levels, respectively.
- **Mapping out potential new standards**. Lastly, we outline some of the research outcomes and advances that could be subject for standardization. This means not only identifying FENTEC innovations that could potentially become a reference for future standards but also those very recent research outcomes whose novelty makes them unsuitable for standardization at this moment. This way, we aim to map out the most promising FENTEC components for standardization that we should focus on in the remainder of this project.

3 Standardization Bodies and Related Organizations

Before embarking on the description of the standardization activities carried out within FENTEC, we provide here an overview of those standardization bodies, organizations and working groups that are leading the standardization effort globally and are relevant to FENTEC.

ISO

ISO, the International Organization for Standardization, is the largest international organization devoted to the promotion of standards. With more than 21 000 International standards, ISO is a popular standardization body with standards published in virtually any domain. ISO is composed of over 250 technical committees working on different areas of research and innovation. Of those technical committees, one is of particularly relevant to FENTEC, the technical committee ISO/IEC JTC 1, jointly led with the IEC. Technical committees are in turn internally organized and divided into subcommittees of which the SC 27 IT on "Security Techniques" is of special interest to FENTEC. Lastly, the subcommittee ISO/IEC JTC 1 SC 27 IT Security Techniques is composed of the following working groups: WG 1 on "Information security management systems", WG 2 on "Cryptography and security mechanisms", WG 3 on "Security evaluation, testing and specification", WG 4 on "Security controls and services", WG 5 on "Identity management and privacy technologies". Since the scope of this standardization subcommittee spans a broad breadth of IT systems and scenarios, the whole body of standards comprised in ISO/IEC JTC 1 SC 27 IT Security Techniques is potentially relevant to the project. In the next section we provide a sub-selection of the most relevant standards for FENTEC.

CEN, CENELEC & ETSI

CEN, CENELEC and ETSI are the three officially recognized European Standardization Organizations. CEN and CENELEC seek to promote the adoption of standards at the European level to ensure the quality and interoperability of different technologies as well as the lawfulness according to European regulation. Composed of the national standards agencies of 33 European countries, they also cooperate with ISO and IEC to reach consensus on standards at the international level. ETSI seeks to develop international standards in the field of ICT technologies. They develop standards on various fields such as the cloud, the Internet of Things, smart applications, wireless systems, smart cards, cyber security or security algorithms, among others.

ENISA

ENISA is not standards organization, but it seeks to improve network and information security in the European Union. To that end ENISA advises and assists the European Commission and the member states on information security, collects and analyses data related to security incidents in the European Union and promotes risk assessment and risk management. ENISA periodically publishes the results of their analyses together with recommendations to raise awareness and contribute to a better understanding of the security risks faced by European industry. Our interest in ENISA is two-fold. On the one hand, they provide valuable advice and recommendations on the development and implementation of technology. On the other hand, they focus on the particular context of the European Union, considering current European legislation and the particularities of the European market.

NIST

NIST could be regarded as the CEN/CENELEC/ETSI equivalent in the United States. Among other activities, NIST produces SRMs that define the features and characteristics that certain technologies should meet. Of particular importance in the domain of cryptography, the NIST has defined the current AES and SHA-3 standards.

4 Adoption of Existing Standards

One of the standardization activities of FENTEC is the adoption and follow-up of existing standards. Adopting existing standards has several advantages for our project. On the one hand, it offers a systematic and organized methodology to tackle development issues central to the solution being designed in the project. Moreover, standards offer a reference terminology that often stems from the consensus of different stakeholders, thus helping us using concepts that are broadly understood and agreed upon outside of our own research communities. On the other hand, the critical evaluation of a standard before deciding whether it is relevant or suitable for our project also provides us opportunities to challenge and put into question standards that may need to be updated or revisited.

The field of FE is still too novel and has not been subject to standardization efforts yet. There are still no standards in FE due to its young age, but for some of the underlaying technologies like lattice-based cryptography, the ice has already been broken (e.g., the IEEE P1363 group working on standard specifications for public-key cryptography included NTRU as a core for a future standard in lattice-based public-key cryptography). Lattice-based crypto is also a very promising primitive for post-quantum cryptography because they are believed to be hard even for quantum adversaries. NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Lattice-based primitives are among the most popular in the completion.

A complete list of standards, which we think are relevant for FENTEC will be presented in the second deliverable of Task 2.4 – the final standardization report (D2.12).

5 Contribution to Current Drafts and Future Standards

In addition to adopting published standards or revising and assessing whether they are suitable for the needs of the project, there is also an opportunity to participate in the standardization process by contributing to standards that are currently in the making or, even further, proposing new standards. Needless to say, the former is a less ambitious task but at the same time and in the context of this project more manageable and realistic. This is due to two main reasons: (1) Current working drafts are a joint effort of several entities and thus do not exclusively depend on our effort and commitment. This means that we can provide input to several standards without the burden of leading and managing them. (2) Most current technologies underlying the envisioned FENTEC solutions involve cutting-edge research not ripe for standardization, making standardization prospects uncertain. Standardization of new technologies is a lengthy process that is not typically possible in the duration of a 3-year project. This is further complicated by the fact that research results and solutions are only produced near the end of the project.

In the remainder of this section we describe how we have invested our efforts in these tasks. We describe our efforts at establishing contact with the standardization community. In this regard, our main result is our liaison with ETSI, which enables us to actively contribute to the working group Cyber and more particularly to one of the current efforts: Guide to Identity Based Encryption. The document will describe the use and application of IBE. The report is intended to allow non-experts in the technology of IBE to be able to gain an understanding of the technology, its domains of application, and its required environment. In addition, the document reviews use of IBE against more common asymmetric encryption schemes (e.g. RSA and ECC schemes), as well as more generalized ABE schemes. A review of algorithms available to implement IBE and their evolution to quantum safe instances will also be covered.

We have also applied for liaison to ISO SC 27 IT on “Security Techniques” and more specifically to WG 2 on “Cryptography and security mechanisms”, but unfortunately our request has not been considered yet despite our continuous efforts. We are still in contact with ISO through representatives from partners of the consortium (e.g., KU Leuven).

6 Conclusions

Standards are important for research and innovation projects like FENTEC for a number of reasons. On the one hand, existing standards help addressing well known problems with what has been adopted and agreed upon by the community as a good solution, which in turn helps encouraging further adoption, prevents compatibility problems and broadens the opportunities for exploitation, among other benefits. On the other hand, contributing to standards gives the opportunity to discuss and challenge our project results with a wider community of experts and researchers, thereby enabling communication across different communities and helping us find better solutions and research outcomes.

In this deliverable we have described the standardization activities carried out by FENTEC so far. We have focused on three main types of activities relevant to standardization: adopting existing standards, engaging with standardization organizations and outlining future contributions to standards currently under development or standards-to-be. We have listed the standardization bodies and similar organizations, which we think are relevant for the technologies in the scope of the project. We have established a formal liaison with ETSI and applied for liaison with ISO. These are, however, preliminary results. While we have engaged with standardization bodies and examined relevant existing standards, a more active role where we use part of our results to inform standardization processes currently underway is expected to take place in the second half of the project.

We truly hope we also get granted a liaison with ISO and would have the opportunity to work also with this very important global standardization organization. We hope that part of our research outcomes enables us to provide helpful feedback to these standards. The potential for standardization of technologies developed in FENTEC seems however bleak. Most of our expected research outcomes would be too novel to have any realistic expectations on standardizing them during the lifetime of the project because standardization is a lengthy process that requires a broad consensus that takes time to achieve. In short, during this first half of the project we have focused on identifying relevant standards and standardization gaps as well as establishing contacts with relevant organizations. During the remaining of this project we plan to contribute in a more active way to current standardization efforts in our research domains.