



FOR IMMEDIATE RELEASE

FENTEC Project: Increasing Trustworthiness of ICT solutions developing Functional Encryption

Madrid, March 2018 - Atos, an international leader in digital services, coordinates a Consortium of 9 partners for the implementation of the project “**F**unctional **E**ncryption **T**Echnologies” (FENTEC for short), a three-year multi-disciplinary, Research and Innovation Action co-funded by the European Commission in the context of Horizon 2020, the EU Framework Programme for Research and Innovation.

Encryption is a method for a user to encode and securely share data over an insecure network. Before the arrival of public key cryptography, the common method to share data in a secure way was to establish a mutual secret key beforehand. This fact might be acceptable for some small organizations, but such a solution is clearly unsustainable for larger networks. Today, public key encryption is a well-established technology commonly used in building solutions for secure web communication, disk encryption and secure software patch distribution but fine-grained, cryptographically regulated, access to data or the program executed on the data is becoming possible thanks to a new broad, versatile and powerful paradigm of encryption systems: the Functional Encryption.

FENTEC's core objective is to develop new Functional Encryption (FE) as an efficient alternative to the all-or-nothing approach of traditional encryption, enabling partial views over encrypted data and effectively enhancing security of complex systems by compartmentalization of data or computation over the data. It addresses the challenge to design general purpose FE supporting the decryption of arbitrary (efficiently computable) functions with novel cryptographic algorithms and hardware concepts within practical metrics, balancing the individual functional, efficiency and security requirements. The project brings together a team of cryptographers, software experts, hardware specialists and IT industry representatives with the aim of developing efficient and innovative FE systems which are application oriented and can be used in a wide range of scenarios. FENTEC will design, develop, implement and demonstrate the usefulness and real-life applications of FE, producing tangible advantages for the whole ICT industry and for stakeholders that need to operate in environments where data confidentiality and privacy is needed, but partial access to the data through external parties is unavoidable. The security, efficiency, expressiveness and versatility of the new FE approach will be showcased in three use-cases:

- Privacy-preserving digital currency, enforcing flexible auditing models
- Data Collection and Local Decision Making
- Privacy-Preserving Statistical Analysis

With an estimated budget of around 4 million euro, FENTEC will develop new application-oriented FE systems able to increase the trustworthiness of the European ICT services and products. The project started on January 2018, coordinated by Atos and with partners: Ecole Normale Supérieure (France), Hochschule Flensburg (Germany), Katholieke Universiteit Leuven (Belgium), University of Helsinki (Finland), Nagravision (Switzerland), XLAB (Slovenia), University of Edinburgh (United Kingdom), Wallix (France).

This project has received funding from the European Commission within the Secure Societies theme of the Horizon 2020 Framework Programme for Research and Innovation (H2020-DS-2016-2017) under grant agreement No 780108. For further information please contact us at: www.fentec.eu