OVERVIEW

FENTEC's core objective is to develop new Functional Encryption (FE) as an efficient alternative to the all-or-nothing approach of traditional encryption. The project brings together a team of cryptographers, software experts, hardware specialists and IT industry representatives with the aim of developing efficient, innovative FE systems which are application-oriented and can be used in a wide range of scenarios.

GOALS

- Design functional encryption systems with varying functional, security, hardware and software requirements
- Implement a unified cryptographic API of Functional Encryption systems
- Validate and demonstrate FENTEC technologies and solutions

CONTACT

www.fentec.eu

contact@fentec.eu

@FENTEC_Project

FENTEC Project

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. The Research Executive Agency is not responsible for any use that may be made of the information it contains.

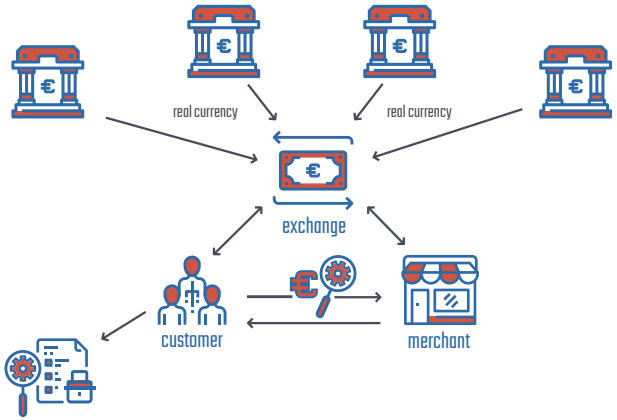
FENTEC

Functional ENcryption TEChnologies

Functional Encryption Technologies

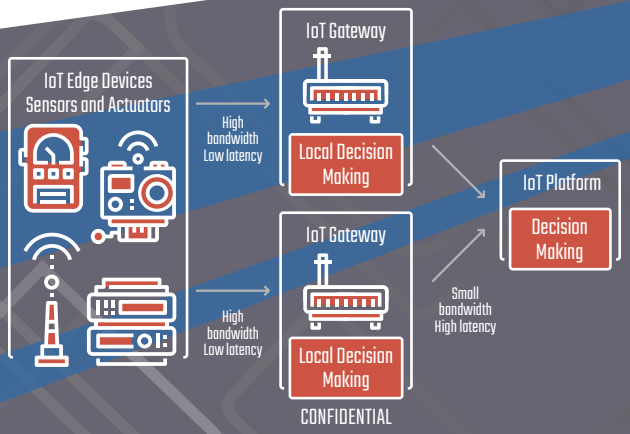
FENTEC is a Research and Innovation Action whose mission is to make the functional encryption paradigm ready for a wide-range of applications, integrating it in ICT technologies as naturally as classical encryption. The primary objective is the efficient and application-oriented development of functional encryption systems. FENTEC's team of cryptographers, software and hardware experts and information technology industry partners will document functional encryption needs of specific applications and subsequently design, develop, implement and demonstrate the applied use of functional cryptography.

Ultimately, a functional encryption library for both SW and HW-oriented applications will be documented and made public so that it may be used by European ICT adopters. With it, the FENTEC team will build emerging security technologies that increase the trustworthiness of the European ICT services and products.



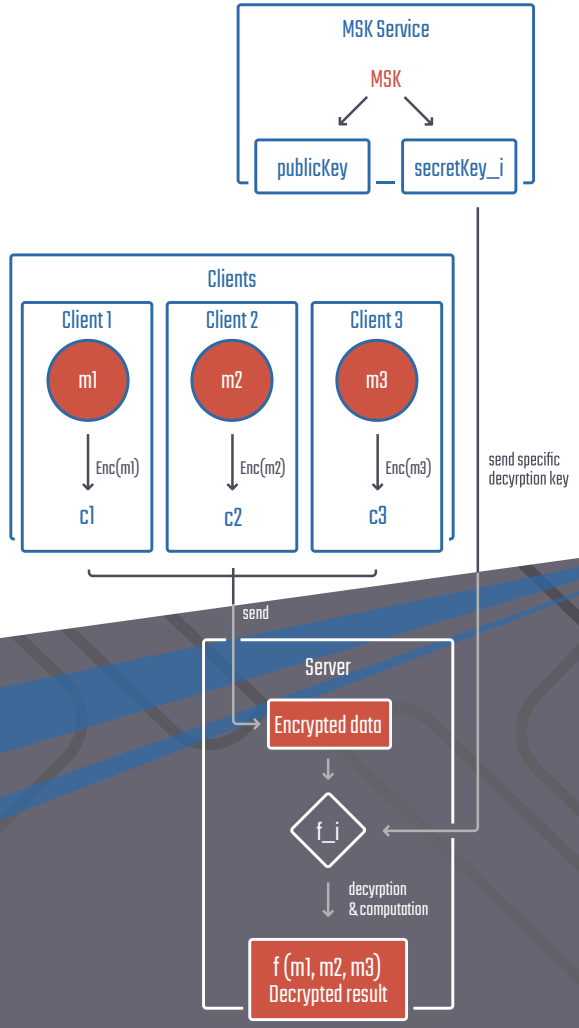
U1. Privacy-preserving and auditable Digital Currency

A digital-based currency as a one-to-one counterpart to physical money, centrally-distributed or issued as convenient as debit and credit cards, but without the related privacy issues.



U2. Data Collection & Local Decision Making

Fentec proposes a new IoT use-case that enables secure Local Decision Making for IoT based on Functional Encryption. The aim is to enable decision making at sub-system level without disclosing end-to-end ciphered data.



U3. Privacy Preserving Statistical Analysis

In this use-case FENTEC addresses the privacy-preserving computation of data analytics. Specifically, the project focuses on the computation of statistics over large usage data. Statistical functions include mean, standard deviation, number, sum and min/max, to name a few examples.