QUANTUM
COMMUNICATION
NETWORKS WORKSHOP

PTQCI
PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

Quantum Random Number Generator Distribution System

Eduardo Fernandes[1,2,*], Maurício J. Ferreira[1,2], Nuno A. Silva[1,2], Armando N. Pinto[1,2], Nelson J. Muga[1]

[1]Instituto de Telecomunicações, Universidade de Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal;
[2]Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal;
***edu.fernandes@ua.pt**

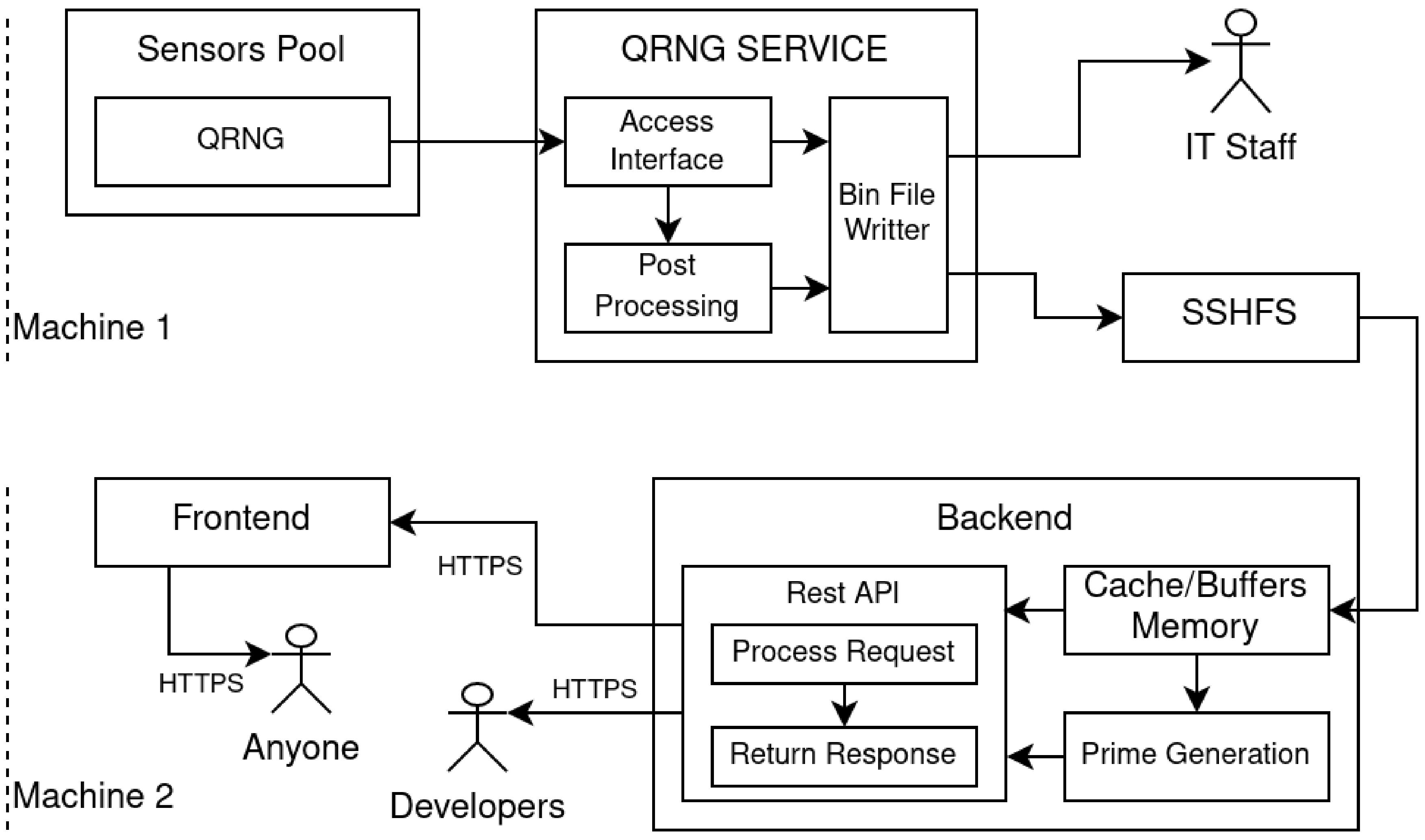
Why the Distribution System

The Distribution System serves a critical role in making available the access to true random numbers generated by us with quantum properties. Through the implementation of the qrng.av.it.pt website, we elucidate the relevance of quantum-based random number generation within the cryptography domain. This platform not only provides a way for disseminating project information but also offers documentation on the utilization of the distributed random and prime numbers. Users are empowered to adapt the output according to their specific requirements, with the system ensuring efficient and fast responses. In summary, the Distribution System serves as a gateway to share the power of quantum randomness, promoting widespread accessibility and utilization within cryptographic applications.

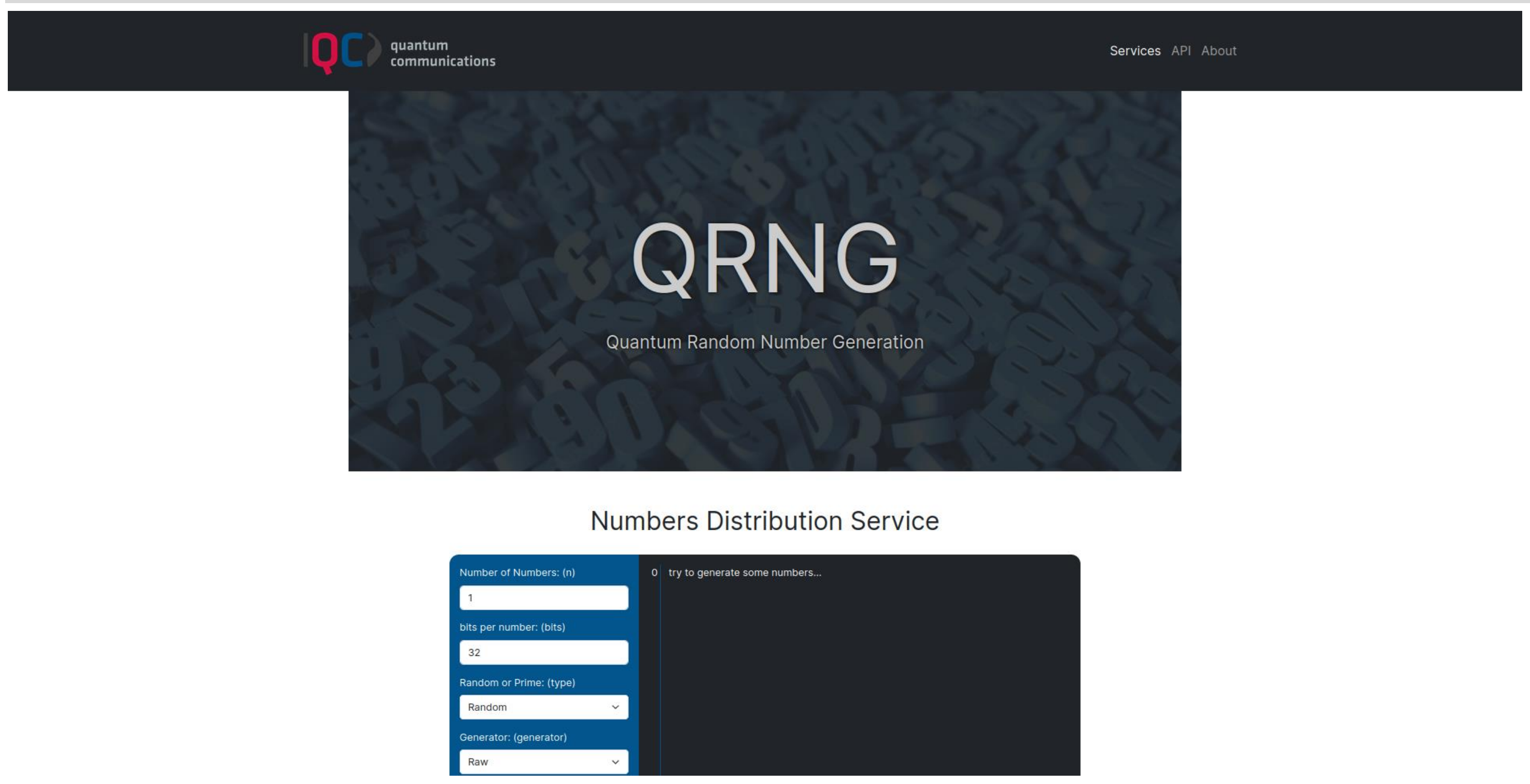
Architecture

The system operates with two machines, with the primary objective of the first machine being to encapsulate extracted random numbers into binary files. These files serve a multitude of purposes and offer versatility in application. The output from the QRNG (Quantum Random Number Generator) contains inherent electrical noise, resulting in the creation of two distinct types of binary files: those with and those without electrical noise. Files containing electrical noise are deemed unsuitable for real-world applications due to the potential predictability they introduce into the data.

The second machine takes on the crucial role of facilitating the accessibility of the generated files over the internet. To ensure a swift and efficient process, these files are read into memory, utilizing buffering techniques. Users are then granted the ability to directly request numbers from the files or opt for on-demand calculations of prime numbers. Serving as the project's entry point for external users, the frontend interface is designed to provide clarity and comprehensive information.



Results



Numbers Distribution Service

Number of Numbers: (n)
1
bits per number: (bits)
32
Random or Prime: (type)
Random
Generator: (generator)
Raw

0 try to generate some numbers...

https://qrng.av.it.pt

- /api/random
  - n = [1, 1000], amount of numbers, default is 1
  - bits = [1, 10000], amount of bits per number, default is 32
  - base = [2, 36], numbers base, default is 10
  - generator = ["pseudo", "raw", "re"], "pseudo" for pseudo-random generated bits, "raw" for numbers quantum generated with eletrical noise, "re" for numbers quantum generated with the eletrical noise removed
- /api/prime
  - n = [1, 100], amount of numbers, default is 1
  - bits = [1, 1024], amount of bits per number, default is 32
  - base = [2, 36], numbers base, default is 10
  - generator = ["pseudo", "raw", "re"], "pseudo" for pseudo-random generated bits, "raw" for numbers quantum generated with eletrical noise, "re" for numbers quantum generated with the eletrical noise removed

Acknowlegments

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under the project QuantumPrime (PTDC/EEI-TEL/8017/2020) and UIDB/50008/2020-UIDP/50008/2020.

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101091730.

Co-funded by the European Union

EuroQCI