CALL FOR APPLICATIONS: RESEARCHER

Job/position/grant:

Job reference:	AE2024-0011 (CentrosTecnInov - HASLAB)
	INESC TEC - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
Job/position/grant:	RESEARCHER
City:	Porto
Research field:	Main: COMPUTER SCIENCE
	Sub: Computer Systems

Job summary:

INESC TEC is accepting applications for 1 RESEARCHER job in the Cyber security

Project:	Funding for Technology and Innovation Centres
Scientific Advisor:	Manuel Barbosa
Start Date:	2024-02-19
Location:	INESC TEC, Porto, Portugal

Job description:

Work Area: Cyber security

Project overview: The overarching goal of this contract is to design, specify and implement a software library that addresses the post-quantum migration needs of eAuthentication systems. This library will contain high-assurance implementations of the relevant PQC cryptographic standards, as well as hybrid protocols that are relevant for the eAuthentication domain. These protocols will be identified based on the requirements identified by ongoing international initiatives in this domain and candidate designs will be formally validated via rigorous cryptographic security proofs.

Objectives: - Analyse existing eAuthentication systems to understand current functional and non-functional requirements;
- Investigate existing guidelines for Post-Quantum Cryptography (PQC) migration that apply to this domain;
- Perform a requirements analysis for the cryptographic components that are needed for eAuthenticayion PQC migration;
- Specify a software library that answers the needs of the eAuthentication domain;
- Identify existing candidate solutions for the identified library components, investigate whether they satisfy the identified requirements and pinpoint gaps in the state-of-the art solutions;
- Employ Computer Aided Cryptography (CaC) methodologies and techniques to address some or all of the above gaps.

Academic Qualifications:	- MSc in Information Security Science.
Minimum profile required:	- Previous experience in demonstrable security of post-quantum cryptographic schemes; - Experience in the area of post-quantum migration.
Preference factors:	- BSc in Informatics Engineering or Computer Science.

Funding Entity:	Co-financed by Component 5 - Capitalization and Business Innovation of core funding for Technology and Innovation Centres (CTI), integrated in the Resilience Dimension of the Recovery and Resilience Plan within the scope of the Recovery and Resilience Mechanism (MRR) of the European Union (EU), framed in the Next Generation EU, for the period 2021 - 2026.
Type of contract:	Uncertain term contract

The hiring shall be governed by what is stipulated in the legislation in force regarding uncertain term employment contracts and by INESC TEC norms.

Selection criteria:	The selection of the candidates will be based on the following criteria, in descending order of consideration: a) Relevant Curriculum in the concerned field of this tender b) Proven experience.
Selection Jury:	President of the Jury: Manuel Barbosa; Member: José Bacelar Almeida; Member: João Marco;
Notification of results:	The results of the selection process will be sent to the interested by electronic mail.
Application period:	From 2024-01-18 to 2024-01-31
Application submission:	Electronic form filling in www.inesctec.pt in the section Work with Us

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU
MI MISSÃO INTERFACE
ANI AGÊNCIA NACIONAL DE INOVAÇÃO