# CALL FOR GRANT APPLICATIONS

# (AE2021-0069)

INESC TEC is now accepting grant applications to award 1 Research Grant (BI) within the scope of the INESC TEC LA funded by National Funds through FCT - Portuguese Foundation for Science and Technology, I.P., project (reference UIDB/50014/2020

## 1. GRANT DESCRIPTION

**Type of grant:** Research Grant (BI)

**General scientific area:** COMPUTER SCIENCE

**Scientific subarea:** Informatics

**Grant duration:** 6 months, starting on 2021-06-01with the possibility of being renewed for a maximum term of one year, in cases where the grant has been awarded to students who are enrolled in non-award courses, or up to two years, in the cases of students enrolled in a master's degree.

**Scientific advisor:** Manuel Barbosa

**Workplace:** INESC TEC, Porto, Portugal

**Maintenance stipend:** € 835,98, according to the table of monthly maintenance stipend for FCT grants, paid via bank transfer. Grant holders may be awarded potential supplements, according to a quarterly evaluation process (Articles 19, 21 and 22 of the Regulations for Grants of INESC TEC and Annex II), up to a maximum limit of 50% of the monthly maintenance stipend.

Costs attributable to INESC TEC may include registration, enrolment or tuition fee stipend, either directly or through reimbursement, during the grant duration.

The grant holder will benefit from health insurance, supported by INESC TEC.

## 2. OBJECTIVES:

The MPC-in-the-Head paradigm allows transforming secure computation protocols into Zero-Knowledge protocols with unique characteristics, not only with respect to their expressiveness, but also because they can guarantee post-quantum security.

The goal of this work will be to prototype zero-knowledge protocols based on the MPC-in-the-Head paradigm in the Jasmin language, to investigate their optimization, and to integrate them into protocols verified in EasyCrypt.

## 3. BRIEF PRESENTATION OF THE WORK PROGRAMME AND TRAINING:

The successful candidate will be integrated in the research team that works in the development of protocols based on the MPC in the Head paradigm, focusing on the implementation, optimization and verification of code written in Jasmin and EasyCrypt. These activities fall within the range of skills in IT security engineering that are developed within the Computer Science Masters Degrees at the University of Porto.

## 4. REQUIRED PROFILE:

**Admission requirements:**

BSc in Informatics Engineering
The awarding of the fellowship is dependent on the applicants' enrolment in study cycle or non-award courses of Higher Education Institutions.

**Preference factors:**

Knowledge in zero-knowledge proofs, MPC-in-the-head, and efficient implementation of cryptography in the Jasmin language.

**Minimum requirements:**

Experience in cryptography and code optimization in low level languages.

## 5. EVALUATION OF APPLICATIONS AND SELECTION PROCESS:

**Selection criteria and corresponding valuation:** the first phase comprises the Academic Evaluation (AC), based on the criteria referred to in Article 12 of the Regulations for Grants of INESC TEC, while the second phase comprehends the Individual Interview (EI). All factors are evaluated on a scale of 0 to 100, taking into account the applicants' merit, suitability and conformity with the preference factors.
The weight of the AC factors are as follows: Academic Qualifications (FA, 50%), Scientific Publications (PC, 15%), Experience (EX, 20%) and Motivation Letter (CM, 15%).
Candidates who score less than 50 points in the AC average will be considered excluded on absolute merit. The top five candidates approved on absolute merit will be qualified for the individual interview. The Final Grade (CF) is obtained by the weighted average of AC (85%) and EI (15%).

**The Selection Jury is composed of the following members:**

President of the Jury: Manuel Barbosa
Full member: José Bacelar Almeida
Full member: Alcino Cunha
Substitute member: Hugo Pereira Pacheco

**Release of results and prior hearing:** the results of the selection process, as well as the terms and procedures for prior hearing, will be released to the applicants by email, under the terms referred to in Article 13 of the Regulations for Studentships and Fellowships of INESC TEC.

## 6. FORMALISATION OF APPLICATIONS:

**Application Documents:**

1. Motivation letter;
2. Curriculum Vitae (must include the list of previous fellowships, their type, beginning and end dates, funding entities and host institutions);
3. Certificate or diploma degree dully recognised in Portugal;
   - Documents proving the awarding of academic degrees and diplomas, or the according recognition - in cases of academic degrees or diplomas granted by a foreign higher education institution - can be dismissed in the application process, and replaced by the applicant's declaration of honour, with the verification of said condition taking place during the grant's hiring stage. The submission of the certificate is mandatory when signing the contract.
   - Academic degrees or diplomas awarded by a foreign higher education institution require an authentication by a Portuguese higher education institution, and the corresponding registration on the DGES platform, in conformity with Decree-Law no. 66/2018, of August 16, and Ordinance no. 33/2019, of January 25. More information available on the website https://www.dges.gov.pt/pt/pagina/reconhecimento?plid=374
4. Proof of enrollment in a degree awarding study cycle or in a non degree awarding Higher Education program.
   - The proof of enrollment may be presented just during the grant hiring stage.
5. Signed declaration stating the infringement of the grant holder's duties (article 14, no. 4)
6. Documental evidence to support the country of residence, residence permit or other legally equivalent document, in cases where the applicant is a foreigner or non-resident in Portugal - valid until the beginning of the grant.
7. Other supporting documents relevant to the final assessment.

Failure to deliver the required documents within the 90-day period after the date of the notice of the conditional awarding of the grant implies its cancellation.

**Application period:** From 2021-03-31 to 2021-04-15

**Submission of applications:** the application will be formalised by submitting the form available in the *Work With Us* section of INESC TEC website.

**7. BINDING LEGISLATION AND REGULATION**

The hiring process shall comply with the current legislation regarding the Research Grant Holder Statute, approved by Law no. 40/2004 of August 18, in its current wording, as well as by the Regulations for Grants of INESC TEC and for FCT Grants Regulation in force.

For more information, please check the Regulations for Grants of INESC TEC and relevant annexes at www.inesctec.pt/bolsas