HORIZON

Call: ERC-2021-STG
(Call for Proposals for ERC Starting Grant)

Topic: ERC-2021-STG

Type of Action: HORIZON-ERC
(HORIZON ERC Grants)

Proposal number: 101039196

Proposal acronym: CRETE

Type of Model Grant Agreement: HORIZON Action Grant Budget-Based

Table of contents

1 - General information

Topic	ERC-2021-STG	Type of Action	HORIZON-ERC
Call	ERC-2021-STG	Type of Model Grant Agreement	HORIZON Action Grant B

Acronym   CRETE

Proposal title   Certified Refinement Types

Note that for technical reasons, the following characters are not accepted in the Proposal Title and will be removed: < > " &

Duration in months*   60

Primary ERC Review Panel*   PE6 - Computer Science and Informatics

Secondary ERC Review Panel   (if applicable)

ERC Keyword 1*   PE6_03 Software engineering, programming languages and systems

Please select, if applicable, the ERC keyword(s) that best characterise the subject of your proposal in order of priority.

ERC Keyword 2   *PE6_03 Software engineering, programming languages and systems*

ERC Keyword 3   *PE6_04 Theoretical computer science, formal methods, automata*

ERC Keyword 4   *Not applicable*

Free keywords   *refinement types, type systems, SMT program verification*

Application forms

Proposal ID **101039196**

Acronym   **CRETE**

Abstract *

Type-theory formal verifiers (e.g., Coq, Agda) have been extensively used to prove program properties (e.g,, compiler correctness).
Such verifiers are carefully designed to implement core systems (variants of Martin-Löf's type theory) that are known to be sound, i.e., if verifier accepts the program, then it generates a mathematical proof.
But, type-theory verifiers are not typically used to develop general purpose programs.
They require explicit proof terms and provide limited support for real program features (like non-termination) rendering real world program development impractical.

Refinement types (e.g., Liquid Haskell and F*) were designed as a practical alternative to type-based verification and have been successfully used to verify real world applications (e.g., memory safety and security policy enforcement).
Such systems start from an actual programming language, extend it with logical predicates to specify properties of the language, and automatically validate these specifications using SMT solvers.
Yet, refinement types suffer from the disadvantage that they do not generate proofs machine checked by a core calculus.
In practise, both Liquid Haskell and F* have many times been found unsound.

The goal of this proposal is the design of a sound and practical refinement type system.

This requires building a verification system that is as practical as refinement types and constructs machine-checked mathematical proofs.
The system will be implemented on refinement types systems of mainstream programming languages (i.e., Haskell and Rust) and will be evaluated on verification of real applications, such as web security and cryptographic protocols.

This proposal is of high risk since it aims to develop a novel program logic in which SMT automation co-exists with real world programming features (e.g., diverging and effectful programs).
Yet, it is of high gain since it will render sound, type-based verification accessible to mainstream program

Remaining characters   9

Has this proposal (or a very similar one) been submitted in the past 2 years in response to a call for proposals under any EU programme, including the current call? *	○ Yes ⦿ No

Please give the proposal reference or contract number.

Application forms

Proposal ID   **101039196**

Acronym   **CRETE**

Declarations

1) We declare to have the explicit consent of all applicants on their participation and on the content of this proposal. * ☒

2) We confirm that the information contained in this proposal is correct and complete and that none of the project activities have started before the proposal was submitted (unless explicitly authorised in the call conditions). ☒

3) We declare:
    - to be fully compliant with the eligibility criteria set out in the call
    - not to be subject to any exclusion grounds under the EU Financial Regulation 2018/1046
    - to have the financial and operational capacity to carry out the proposed project. ☒

4) We acknowledge that all communication will be made through the Funding & Tenders Portal electronic exchange system and that access and use of this system is subject to the Funding & Tenders Portal Terms and Conditions. ☒

5) We have read, understood and accepted the Funding & Tenders Portal Terms & Conditions and Privacy Statement that set out the conditions of use of the Portal and the scope, purposes, retention periods, etc. for the processing of personal data of all data subjects whose data we communicate for the purpose of the application, evaluation, award and subsequent management of our grant, prizes and contracts (including financial transactions and audits). ☒

6) We declare that the proposal complies with ethical principles (including the highest standards of research integrity as set out in the ALLEA European Code of Conduct for Research Integrity, as well as applicable international and national law, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Appropriate procedures, policies and structures are in place to foster responsible research practices, to prevent questionable research practices and research misconduct, and to handle allegations of breaches of the principles and standards in the Code of Conduct. ☒

7) We declare that the proposal has an exclusive focus on civil applications (activities intended to be used in military application or aiming to serve military purposes cannot be funded). If the project involves dual-use items in the sense of Regulation 428/2009, or other items for which authorisation is required, we confirm that we will comply with the applicable regulatory framework (e.g. obtain export/import licences before these items are used). ☒

8) We confirm that the activities proposed do not
    - aim at human cloning for reproductive purposes;
    - intend to modify the genetic heritage of human beings which could make such changes heritable
      (with the exception of research relating to cancer treatment of the gonads, which may be financed), or
    - intend to create human embryos solely for the purpose of research or for the purpose of stem
      cell procurement, including by means of somatic cell nuclear transfer.
    - lead to the destruction of human embryos (for example, for obtaining stem cells)
These activities are excluded from funding. ☒

9) We confirm that for activities carried out outside the Union, the same activities would have been allowed in at least one EU Member State. ☒

The coordinator is only responsible for the information relating to their own organisation. Each applicant remains responsible for the information declared for their organisation. If the proposal is retained for EU funding, they will all be required to sign a declaration of honour.

False statements or incorrect information may lead to administrative sanctions under the EU Financial Regulation.

2 - Participants

List of participating organisations

#	Participating Organisation Legal Name	Country	Action
1	FUNDACION IMDEA SOFTWARE	Spain	

2 - Participants

Application forms

Proposal ID **101039196**

Acronym **CRETE**

Short name **IMDEA SOFT**

Organisation data

Host Institution

PIC	Legal name
998520426	*FUNDACION IMDEA SOFTWARE*

Short name: IMDEA SOFT

Address

Street   CAMPUS DE MONTEGANCEDO SN

Town   POZUELO DE ALARCON

Postcode   28223

Country   Spain

Webpage   www.software.imdea.org

Specific Legal Statuses

Legal person	no
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME **(small- and medium-sized enterprise) for the call.**

SME self-declared status.....................................	14/02/2007 - no
SME self-assessment	unknown
SME validation sme	unknown

Proposal ID   **101039196**

Acronym   **CRETE**

Short name   **IMDEA SOFT**

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below?   ○ Yes   ◉ No

Minimum requirements (building blocks) for a GEP

Public GEP: formal document published on the institution's website and signed by the top management, addressing the following issues:

- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel and students and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Minimum areas** to be **covered** and addressed via concrete measures and targets:
    o work-life balance and organisational culture;
    o gender balance in leadership and decision-making;
    o gender equality in recruitment and career progression;
    o integration of the gender dimension into research and teaching content;
    o measures against gender-based violence including sexual harassment.

Application forms

Proposal ID **101039196**

Acronym **CRETE**

Short name **IMDEA SOFT**

Departments carrying out the proposed work

Department 1

Department name	IMDEA Software Institute	☐ not applicable
	☒ Same as proposing organisation's address	
Street	CAMPUS DE MONTEGANCEDO SN	
Town	POZUELO DE ALARCON	
Postcode	28223	
Country	Spain	

Application forms

Proposal ID   **101039196**

Acronym   **CRETE**

Short name   **IMDEA SOFT**

Principal Investigator

The following information of the Principal Investigator (PI) is used to personalise the communications. The EU services will contact the PI together with the HI contact person concerning this proposal (e.g. for additional information, invitation to interviews, sending of evaluation results, convocation to start grant preparation). Please make sure that your personal information is accurate and please inform the ERC in case your e-mail address changes by using the call specific e-mail address indicated in the below webpage. Please also provide your mobile phone number as we may need to urgently contact you regarding your submitted proposal and/or potential interview.

https://erc.europa.eu/about-erc/contact-us

The name and e-mail of contact persons including the Principal Investigator, Host Institution contact are read-only in the administrative form, only additional details can be edited here. To give access rights and contact details of contact persons, please save and close this form, then go back to Participants Step of the submission wizard and save the changes.

ORCID	0000-0001-9112-548X

Researcher ID				*The maximum length of the identifier is 11 characters (ZZZ-9999-2010) and the minimum length is 9 characters (A-1001-2010).*

Other ID	NIE	Y6865305A

Career Stage	Category C Recognised researcher

Last Name*	Vazou	Last Name at Birth	Vazou
First Name(s)*	Niki	Gender*	○ Male ● Female ○ Non Binary
Title	Dr.	Country of residence	Spain
Nationality*	Greece	Country of Birth*	Greece
Date of Birth* (DD/MM/YYYY)	20/07/1987	Place of Birth*	Cholargos

Contact address

Current organisation name	Fundacion IMDEA Software
Current Department/Faculty/Institute/ Laboratory name	IMDEA Software Institute

☒ Same as organisation address

Street	CAMPUS DE MONTEGANCEDO SN		
Postcode/Cedex	28223	Country*	Spain
Town*	POZUELO DE ALARCON		
Phone	+34911012202	Phone2 / Mobile	+34666821182
E-mail*	niki.vazou@imdea.org		

Application forms

Proposal ID **101039196**

Acronym **CRETE**

Short name **IMDEA SOFT**

Contact address of the Host Institution and contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mrs

Gender ⦿ Woman ◯ Man ◯ Non Binary

First name* **Maria**   Last name* **Alcaraz**

E-Mail* **p-maria.alcaraz@software.imdea.org**

Position in org. General Manager

Department FUNDACION IMDEA SOFTWARE   ☒ Same as organisation name

☒ Same as proposing organisation's address

Street CAMPUS DE MONTEGANCEDO SN

Town POZUELO DE ALARCON   Post code 28223

Country Spain

Website https://software.imdea.org/index.html

Phone +34911012202   Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Juan Jose	COLLAZO NIETO	juanjose.collazo@imdea.org	*+34911012202*
Teresa	Gimenez	teresa.gimenez@imdea.org	*+34911012202*

Application forms

Proposal ID **101039196**

Acronym **CRETE**

3 - Budget

?

Beneficiary Short Name	PI	Senior Staff	Postdocs	Students	Other Personnel costs	A. Total personnel costs/€	B. Subcontracting Costs/€ (No indirect costs)	C.1 Travel and subsistence	C.2 Equipment - including major equipment	Consum-ables incl. fieldwork and animal costs	Publications (incl. Open Access fees) and dissemination	Other additional direct costs	C.3 Total other goods, works and services	Total Purchase costs/€	D. Internally invoiced goods and services/€ (No indirect costs)	E. Indirect Cost/€	Total Eligible Costs	Requested EU contribution /€
Imdea Soft	286327	0	266857	420872	140291	1114347.00	0	77653	0	0	5000	3000	8000.00	85653.00	0	300000.00	1500000.00	1500000.00
Total	286327	0	266857	420872	140291	1114347.00	0	77653	0	0	5000	3000	8000.00	85653.00	0	300000.00	1500000.00	1500000.00

Section C. Resources (Maximum 8000 characters allowed)

?

C.1. Research Environment.

The project will be carried out at the IMDEA Software Institute, a research institute promoted by the Madrid Regional Government to perform research of excellence in software development technologies.
The Institute has an international character, with 75% of the faculty having obtained their PhDs outside of Spain.
The PI is part of the Reliable Concurrent Software Group, which covers the domains of Program Analysis and Verification and Languages, Compilers, and Systems.
To sustain the large extent of the project we will also leverage our extensive network of international collaborations, which includes leading experts on topics relevant to the objectives of CRETE.
Specifically, our collaboration plan includes, among others Leonidas Lampropoulos (University of Maryland) on certificate testing; Alex Kavvos (University of Bristol) and Michael Greenberg (Pomona College) on the development of the refinement logic and translation to Coq; Gilles Barthe (MPI-SP) on applications for cryptographic protocols; Ranjit Jhala, Nadia Polikarpova, Deian Stefan (UC San Diego) and Michael Hicks (University of Maryland) on applications for web security.
We also also plan to continue close collaboration with Andres L?h, a Haskell Consultant at Well-Typed LLP, to ensure that the results of CRETE are useful to mainstream developers.

C.2 The project research group.

The CRETE project will include the PI (75% dedication, 286.327 ?), one postdoctoral researcher (PDoc, 5 years; 266.857 ?), three PhD students (PhD-1, PhD-2, PhD-3; 4 years each; 420.872 ? in total), and one research engineer (RE; 4 years; 140.291 ?).
The postdoctoral appointments at IMDEA last between 2 to 4 years, so the position will be split between 2 people depending on the availability of qualified candidates.
RE is included under "other personnel costs".

The Gantt chart of CRETE is summarised in Figure 3 of Section B.
The PI, together with the PDoc will be involved in all research tracks and will be responsible both for track integration (e.g., to ensure that the formalization developed in research track II properly models the implementation of research track IV) and student supervision.
The three PhD students will deliver their doctoral theses following, respectively, the first three tracks of CRETE:
- PhD-1 will work on research track I to design, validate and test certified refinement types;
- PhD-2 will work on research track II and will formalise the logic of refinement types; and
- PhD-3 will work on research track III and will translate certified refinements to type theory.

The RE will join the project in the first or second year of CRETE, depending on the candidate's availability.
The RE, in coordination with the PI will focus on the maintenance and engineering requirements of Task IV.1.

The PI, together with her current PhD student, who is founded by IMDEA, has already initiated the development of the Liquid Rust verifier that is part of Task IV.2.
The results of this development will merge with the certification methodology developed in CRETE.

Local collaborators.
We will also leverage our local connections at IMDEA Software.
Specifically, we plan to collaborate with Aleksandar Nanevski on the Coq derivation; Marco Guarnieri on security applications; and Dario Fiore on the verification of cryptographic protocols.

Collaboration program.
We will maintain our international collaborations mentioned before.
According to the on-going work we will invite some of our colleagues to collaborate on specific topics related to the project.

One of our main goals will be disseminating our results, so for this reason we include 5.000 ? for open access publications costs and, in addition, 77.653 ? for travel costs.
These travel costs include the attendance of the project team to international scientific events to present the projects results, the visits to our external colleagues,
as well as the costs for external collaborators who will be visiting the IMDEA Software Institute.
As we don't know how the evolution of the travel restrictions will be in the incoming years, this travel budget is a conservative estimation based on our experience.
At any case we foreseen that IMDEA can provide us support by covering part of the travel costs.
Finally we claim 3.000 ? under the "other additional direct costs" category for the final financial audit.

Remaining characters 3510

4 - Ethics & security

Ethics Issues Table

1. Human Embryonic Stem Cells and Human Embryos			Page
Does this activity involve Human Embryonic Stem Cells (hESCs)?	○ Yes	⦿ No	
Does this activity involve the use of human embryos?	○ Yes	⦿ No	

2. Humans			Page
Does this activity involve human participants?	○ Yes	⦿ No	
Does this activity involve interventions (physical also including imaging technology, behavioural treatments, etc.) on the study participants?	○ Yes	⦿ No	
Does this activity involve conducting a clinical study as defined by the Clinical Trial Regulation (EU 536/2014)? (using pharmaceuticals, biologicals, radiopharmaceuticals, or advanced therapy medicinal products)	○ Yes	⦿ No	

3. Human Cells / Tissues (not covered by section 1)			Page
Does this activity involve the use of human cells or tissues?	○ Yes	⦿ No	

4. Personal Data			Page
Does this activity involve processing of personal data?	○ Yes	⦿ No	
Does this activity involve further processing of previously collected personal data (including use of preexisting data sets or sources, merging existing data sets)?	○ Yes	⦿ No	
Is it planned to export personal data from the EU to non-EU countries? Specify the type of personal data and countries involved	○ Yes	⦿ No	
Is it planned to import personal data from non-EU countries into the EU or from a non-EU country to another non-EU country? Specify the type of personal data and countries involved	○ Yes	⦿ No	
Does this activity involve the processing of personal data related to criminal convictions or offences?	○ Yes	⦿ No	

5. Animals			Page
Does this activity involve animals?	○ Yes	⦿ No	

6. Non-EU Countries			Page
Will some of the activities be carried out in non-EU countries?	○ Yes	⦿ No	
In case non-UE countries are involved, do the activities undertaken in these countries raise potential ethics issues?	○ Yes	⦿ No	
It is planned to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?	○ Yes	⦿ No	
Is it planned to import any material (other than data) from non-EU countries into the EU or from a non-EU country to another non-EU country? For data imports, see section 4.	○ Yes	⦿ No	
Is it planned to export any material (other than data) from the EU to non-EU countries? For data exports, see section 4.	○ Yes	⦿ No	
Does this activity involve low and/or lower middle income countries, (if yes, detail the benefit-sharing actions planned in the self-assessment)	○ Yes	⦿ No	
Could the situation in the country put the individuals taking part in the activity at risk?	○ Yes	⦿ No	

7. Environment, Health and Safety			Page

Application forms

Proposal ID **101039196**

Acronym   **CRETE**

Does this activity involve the use of substances or processes that may cause harm to the environment, to animals or plants.(during the implementation of the activity or further to the use of the results, as a possible impact) ?	○ Yes ◉ No
Does this activity deal with endangered fauna and/or flora / protected areas?	○ Yes ◉ No
Does this activity involve the use of substances or processes that may cause harm to humans, including those performing the activity.(during the implementation of the activity or further to the use of the results, as a possible impact) ?	○ Yes ◉ No

8. Artificial Intelligence	Page
Does this activity involve the development, deployment and/or use of Artificial Intelligence? (if yes, detail in the self-assessment whether that could raise ethical concerns related to human rights and values and detail how this will be addressed).	○ Yes ◉ No

9. Other Ethics Issues	Page
Are there any other ethics issues that should be taken into consideration?	○ Yes ◉ No

I confirm that I have taken into account all ethics issues above and that, if any ethics issues apply, I will complete the ethics self-assessment as described in the guidelines How to Complete your Ethics Self-Assessment   ⊠

Application forms

Proposal ID **101039196**

Acronym   **CRETE**

Ethics Self-Assessment

Ethical dimension of the objectives, methodology and likely impact
Describe how the issue(s) identified in the ethics issues table above will be addressed in order to adhere to the ethical principles and what will be done to ensure that the activities are compliant with the EU/national legal and ethical requirements of the country or countries where the tasks are to be carried out. It is reminded that for activities performed in a non-EU countries, they should also be allowed in at least one EU Member State.

Compliance with ethical principles and relevant legislations
Describe how the issue(s) identified in the ethics issues table above will be addressed in order to adhere to the ethical principles and what will be done to ensure that the activities are compliant with the EU/national legal and ethical requirements of the country or countries where the tasks are to be carried out. It is reminded that for activities performed in a non-EU countries, they should also be allowed in at least one EU Member State.

Application forms

Proposal ID   **101039196**

Acronym   **CRETE**

Security issues table

1. EU Classified Information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?	○ Yes	◉ No	
Does this activity involve non-EU countries?	○ Yes	◉ No	

2. Misuse			Page
Does this activity have the potential for misuse of results?	○ Yes	◉ No	

3. Other Security Issues			Page
Does this activity involve information and/or materials subject to national security restrictions? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	◉ No	
Are there any other security issues that should be taken into consideration? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	◉ No	

[2]According to the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, "European Union classified information (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States".

[3]Classified background information is information that is already classified by a country and/or international organisation and/or the EU and is going to be used by the project. In this case, the project must have in advance the authorisation from the originator of the classified information, which is the entity (EU institution, EU Member State, third state or international organisation) under whose authority the classified information has been generated.

[4]EU classified foreground information is information (documents/deliverables/materials) planned to be generated by the project and that needs to be protected from unauthorised disclosure. The originator of the EUCI generated by the project is the European Commission.

Application forms

Proposal ID **101039196**

Acronym **CRETE**

5 - Other questions

Academic data	
PhD reference date	
Date of earliest award (PhD or equivalent) - DD/MM/YYYY*	10/12/2016
Applicants holding a Medical degree	
Are you a medical doctor or do you hold a degree in medicine? Please note that if you have also been awarded a PhD, your medical degree may be your first eligible degree. (please see the ERC Information for Applicants to the Starting and Consolidator Grant for more details).	○ Yes ◉ No
Extension Requests	
With respect to the earliest award (PhD or equivalent), I request an extension of the eligibility window, (indicate number of days) [see the applicable ERC Work Programme and the Information for Applicants to the Starting and Consolidator Grant Call].	○ Yes ◉ No
Working time commitment	
Please indicate your percentage of working time in an EU Member State or Horizon Europe Associated Country over the period of the grant. Please note that you are expected to spend a minimum of 50% of your total working time in an EU Member State or Associated Country.*	100
Please indicate the % of working time you (as PI) will dedicate to the project over the period of the grant. Please note that PIs are expected to dedicate a minimum of working time to the project (30% for AdG, 40% for CoG and 50% for StG). The personnel cost for the PI provided in section "3-Budget" cannot be higher than the percentage indicated here. This information will be provided to the experts at Step 2 together with the section "3-Budget".*	75
ERC eligibility requirements	
Please acknowledge that you are aware of the eligibility requirements for applying for this ERC call as specified in the ERC Annual Work Programme, and please certify that, to the best of your knowledge your application is in compliance with all these requirements. Please note that your proposal may be declared ineligible at any point during the evaluation or granting process if it is found not to be compliant with these eligibility criteria.*	☒
Consent obtained from participants and researchers	
Please confirm that you (as PI) have the written consent of all participants on their involvement and the content of this proposal, as well as of any researcher mentioned in the proposal on their participation in the project (either as team member, collaborator, other PI or member of the advisory board). We may request you to provide proof of the written consent obtained at any time during the evaluation.*	☒
Sharing evaluation data	
If your proposal is not funded (due to budget limitations), do you consent to allow us to disclose the results of your evaluation (score and ranking range), together with your name (as PI), non-confidential proposal title, acronym, abstract and your/your host institution's contact details to national or regional public research funding authorities that run funding schemes specifically for ERC applicants that scored highly in the evaluation?	◉ Yes ○ No

Application forms

Proposal ID **101039196**

Acronym   **CRETE**

If your proposal is funded, do you consent to allow us to disclose your name (as PI), non-confidential proposal title, acronym, abstract and your/your host institution's contact details to institutions that are awarding prizes to excellent researchers?	⦿ Yes ○ No

Application forms

Proposal ID **101039196**

Acronym   **CRETE**

Excluded Reviewers

You can provide up to three names of persons that should not act as an evaluator in the evaluation of the proposal for potential competitive reasons.

First Name	Derek
Last Name	Dreyer
Institution	Max Plank Institute (MPI-SWS)
Town	Saarbruecken
Country	Germany
Webpage	https://people.mpi-sws.org/~dreyer/

Excluded Reviewers