



13 Sep 2021

## NGIatlantic.eu third Open Call: applications and winning proposals!

13 Sep 2021

*13 September 2021*

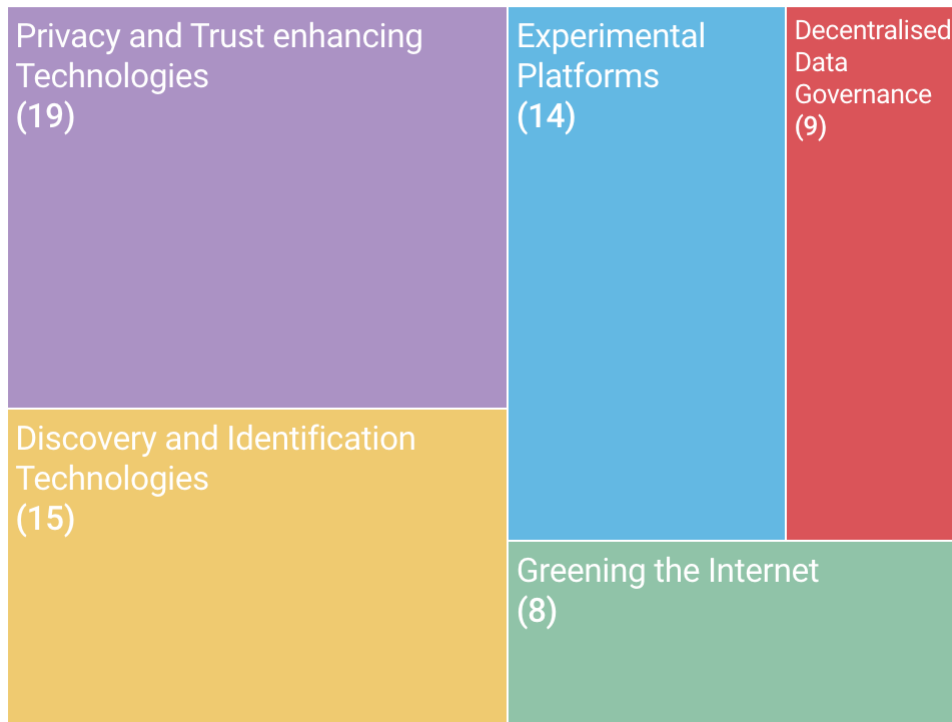
The H2020 project [NGIatlantic.eu](https://ngiatlantic.eu) supports collaboration on NGI topics between the EU and the US through a set of 5 Open Calls for funding, with a total budget of 2.8 Million euro to incentivise EU – US NGI teams to carry out joint experiments using EU and/or US based experimental platforms.

The 3rd Open Call focused on two main categories of topic. The first, stream a) was devoted to **EU – US Experimental Platforms interconnection** and therefore, invited established designers and facility providers of experimental infrastructures, testbeds, and platforms which could be used for experiments in NGI areas on both sides of the Atlantic to interconnect and to offer their facilities on a continuous basis to the community of experimenters and application developers in other NGI topics.

The second, stream b) was dedicated to **NGI Priority topics where results are already available for experimentation on EU – US platforms**. The focus on this part of the call was to take results from topics already in a mature state in the related priority topics of the NGI initiative to the next stage of experimentation of results on EU – US experimental platforms. Two new topics have been added to this category, compared to the previous calls, also on the basis of recommendations of the project's EU – US External Advisory Group (EAG).

The images below provide a statistical overview of the topics covered by applications to the 3rd Open Call and the funded EU-US experiments:

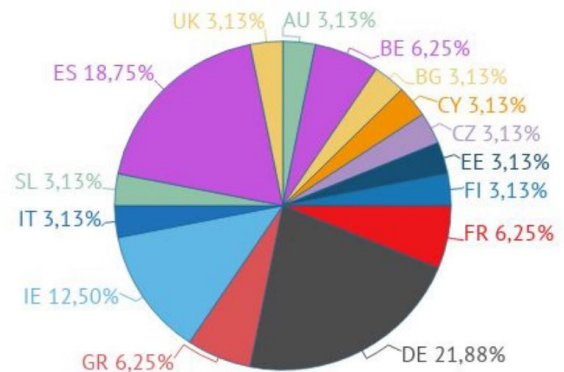
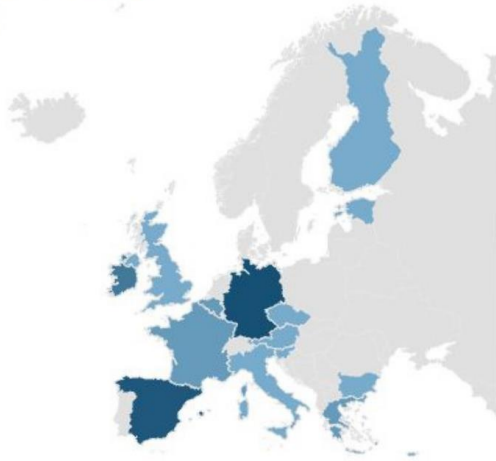
# Topics coverage



A total of 32 applications were made to the 3rd Open Call. Applications were submitted by coordinators from 15 different EU countries and 16 different US partner States. Each proposal was evaluated based on 4 criteria: (1) Soundness of the proposal and foreseen impact on the Open Call topic; (2) Technical excellence & adherence to the Open Call topics; (3) Experience and qualifications of the applicant; (4) Economics of the proposal.

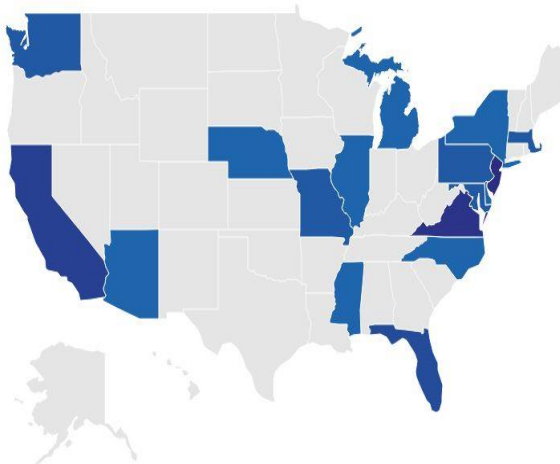
## PROJECT COORDINATORS COUNTRIES

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czechia
- Estonia
- Finland
- France
- Germany
- Greece
- Ireland
- Italy
- Slovenia
- Spain
- United Kin



## US Partner States

- Arizona
- California
- Delaware
- Florida
- Illinois
- Maryland
- Massachusetts
- Mississippi
- Missouri
- Nebraska
- New Jersey
- New York
- North Carolina
- Pennsylvania
- Virginia
- Washington



NGIatlantic.eu is happy to announce that nine of these projects have been selected for the third Open Call, with a total funding budget of 662.199 €:

## Here are some abstracts from our 9 winning projects!

1: ATLANTIC-eVISION: Cross-Atlantic Experimental Validation of Intelligent SDN-controlled IoT Networks



[Technological University of Dublin](#) and [University College of Dublin](#) with [University of Nebraska](#)

The project by the Technological University of Dublin and the University College of Dublin (EU) with the University of Nebraska (US), addresses the NGI topic of “Discovery and identification technologies” with the aim of setting up experiments in real testbeds for the first time, for the automatic discovery of wireless IoT nodes using SDN/OpenFlow. Traditionally OpenFlow is suited to fixed networks. Some efforts have already been made to extend the application of OpenFlow in wireless networks: the novelty in this case is the automatic IoT node discovery using OpenFlow combined with machine-learning-based intelligence and applied over an intercontinental testbed. Experiments will be carried out on real testbeds with enhanced capabilities like COSMOS, POWDER/RENEW, AERPAW and Fed4Fire. This proposal has the potential to revolutionise the way wireless ad-hoc networks can be managed and to pave the way for scalable, low-cost, self-configurable and programmable future IoT networks supporting a plethora of use cases.

## 2: Transatlantic SSI Interop

### Danube Tech GMBH with Digital Bazaar

The concept behind this project is to conduct experiments in the area of the emerging Self-Sovereign Identity (SSI) concept, building on top of infrastructures that are being developed in the US and the EU. SSI is clearly emerging as a next-generation paradigm for digital identity that enables independence, privacy, security, and human dignity for individuals, as well as new opportunities for digital identity of organizations and things. This approach is based on inherently decentralized architectures that eliminate dependencies on centralized authorities. At the moment, and in strong contrast to the ideology of SSI and its foundational technical building blocks, many SSI projects and initiatives built across the world are essentially being designed and deployed in an isolated manner, not interacting with other related efforts. The Danube Tech (EU) and Digital Bazaar (US) team will conduct experiments that connect SSI infrastructures in the US and the EU, with the aim to demonstrate that decentralized digital identity based on open standards can be globally interoperable and connected.





### 3: Physical Unclonable Functions for Identification of Large Scale distributed IoT Assets



#### Asvin GmbH with East Carolina University

Bootstrapping and maintaining fleets of IoT Devices requires automated and secure procedures to process the Identity of Devices, add them to domain controllers and define the trust level in operations. New concepts for bootstrapping of IoT devices are needed due to the weakness of existing procedures in the context of large scale deployments and industry specific constraints by edge operations. Centralized legacy systems and internet protocols are often failing by security, trust and scalability when they are applied to IoT bootstrapping problems. This experiment will test new decentralized architectures and protocols on large scale distributed networks to fix the challenges of secure bootstrapping, identification and management of IoT devices at the edge. The experiment is using US/EU BRIDGES testbed infrastructure and is addressing the call topic on Discovery and Identification technologies in the area of industrial IoT cybersecurity solutions developed by the SME asvin.

### 4: Experimental Assessment of Fast Quantum Key Distribution

#### Universitat Politècnica de Catalunya with University of California

This project addresses the NGI priority topics of Privacy and Trust enhancing technologies with a method which has the expected impact of maximising system performance, thus facilitating the

deployment of Quantum Key Distribution systems to provide long-term data protection in a post-quantum world, by reducing the cost of Quantum Key Distribution systems. The method consists of an AI-based SOP compensator and an augmented key distillation. For this collaboration, the EU-US Experimental Quantum Communication Laboratory (EQC Lab) will be set up, leveraging the extensive experimental research facilities available within the UC Davis NGNCS laboratories.



## 5: Secure communication based on robust 3D localization



### Technical University of Crete with Florida Atlantic University - Center for Connected Autonomy & Artificial Intelligence

The project deals with the implementation and experimentation of secure communication solutions for mobile wireless networks, building on the development of robust 3D localization algorithms. The aim is to enhance the security level of 5G wireless networks which are based on massive MIMO base stations and MIMO client nodes. As a key requirement for 5G wireless systems, security enhancement is among the NGI priority topics and specifically the domain of Privacy and Trust-enhancing technologies. The proposed secure information transmission systems the team will experiment on the POWDER/RENEW testbed will enhance system security and offer solutions to location-aware mobility applications, power allocation and power savings for the mobile terminals, efficient spectrum utilization and sharing, and privacy of data that are uploaded or downloaded by mobile users, especially by the cell-edge ones. In particular, the advances established over the proposed testbed experimentation will satisfy the increased privacy requirements of 5G networks, even when (in contemporary or future networks) eavesdroppers are equipped with powerful computational devices. The implementation, experimentation, and validation of these concepts will allow their regulation in the new mobile communications standards.



## 6: Inclusive verification of cross-border and level of assurance-dependent digital credentials

**SICPA Spain S.L.** with **iRespond Global Inc.**

In the digital world, verification of the legitimate owner of the credentials using a multi-source of information is needed to avoid impersonation issues: the rise of self-sovereign identity and trust framework is a big opportunity in this context. The objective of this project is to delegate access to verifiable credentials and identity to trusted third parties (e.g. decentralized identifiers, eIDAS electronic seal, biometrics etc.), while preserving privacy and meeting the EU regulations (e.g. data minimization, purpose limitation, transparency and confidentiality).

The aim is to replace mobile phones by a cloud agent for the storage of verifiable credentials. The access to this latest will be triggered by secure factors of authentication that citizens will have to demonstrate control over at the point of verification. The verification mechanism should be secure, seamless, preserving data-privacy, inclusive and meet different levels of assurance requirements. The benefits of such a concept are to allow Europe and USA to rely on digital credentials issued by one of the two governments, without having necessarily aligned regulations, data-privacy policies, common identity infrastructure or similar security and level of assurance requirements. Other key benefits are to facilitate the digital transformation of the society, to boost the local economy thanks to trustworthy online transactions and to contribute to the globalization of trust that will enable governments to reuse trusted credentials to issue new credentials.



## 7: Deployment and Evaluation of a 5G Open Spatial Computing Platform in a Dense Urban Environment



### Open AR Cloud with WINLAB and COSMOS

Spatial computing is a broad term for a suite of technologies that result in users being immersed, engaged, and interacting with spatial and temporal digital information that pertain to the physical space in, around, and near the user. It consists of a superset of technologies required for traditional augmented reality. The Open AR Cloud (OARC) association, dedicated to the development of technologies and standards for open and interoperable spatial computing components on which an ecosystem of companies and their services can flourish, has already designed and implemented important building blocks of an Open Spatial Computing Platform (OSCP). The project will replicate the proven components of the OSCP (currently implemented only in European testbeds) on the US-based COSMOS research platform and permit experiments to increase maturity and features of the OSCP components and to demonstrate the OSCP functionality and benefits to more diverse US-based target audiences. The experiments to be conducted are relevant to key NGI enabling technologies including but not limited to 5G, IoT, Big Data and Next Generation Media. All these technologies are fundamental to the research goals and vision of OARC for the future. The proposed NGI experiments would provide the first-ever qualitative and quantitative study of the OSCP components in 5G-enabled campus environments. Using the edge cloud resources and architecture, the project will permit the study of seamlessly updating and changing the 3D map of the real world to which a moving user's queries are sent.

## 8: EdgeFlooding: Exploiting Edge computing for Real-Time Monitoring and Detection of Flash Floods

[University of Pisa - Department of Information Engineering](#) with [University of Maryland Baltimore County - UMBC](#)

The goal of the EdgeFlooding experiment is to assess the feasibility of adopting a Cloud/Edge computing approach for the implementation of the flood monitoring system developed at UMBC. The University of Pisa and the University of Maryland aims at assessing the feasibility of implementing the image and data analysis of the system in a distributed manner, where image and data analysis is performed at the Edge level directly in proximity of the monitoring station, while social media analysis is performed at the Cloud level. Results from the analysis performed at the Edge layer are transmitted to the Cloud in order to obtain a global view (e.g. for regional monitoring) and to implement training and optimization functions to increase the accuracy of the models deployed at the Edge layer. In details, by extending the current implementation of the flood monitoring system and by running a set of real experiments, the team aims at verifying the feasibility of implementing the image and analysis algorithms directly on the Edge nodes, and at measuring metrics such as latency and bandwidth for data transmission between Edge and Cloud to assess their compatibility with a real implementation.



## 9: Adaptive decentralized federated learning in wireless mesh network (FLESHNET)



[Universitat Politècnica de Catalunya](#) with [Mississippi State University](#) and [University of Michigan](#)

The increase of the computing capacity of end user-owned devices and the appearance of lightweight machine learning frameworks have led to the situation that machine learning is nowadays available at user devices, while just a few years ago machine learning was exclusive to cloud providers. The FLESHNET project envisions novel federated learning applications organized as a Peer-to-Peer network in which any worker can participate in the provision of data and in the training of machine learning models. For this to happen, federated learning building blocks must be extended and evaluated. These building blocks will integrate data sovereignty, enable the autonomy of the participants for taking self-determined decisions, facilitate the ownership of machine learning models and data, and enable decentralized governance of the data. This scenario will be realistic in the near future as any peer in a federated learning network will receive an ever increasing amount of data coming from more and more nearby sensors.

Our next Call opens in December, are you interested in receiving updates? Follow us on [Twitter](#) and [LinkedIn](#).