ARCADIA applications are based on a micro-service model and are governed by a sophisticated policy manager. Each ARCADIA application consists of several autonomous components, which can communicate with each other based on a service graph and policy rules defined by the developers. Each component can be stored in a public or private registry on the ARCADIA platform and it can be re-used on other applications.

Internet of Things applications can take ad-vantage of the different features of the ARCADIA framework. For example, by using policies, metrics and re-configuration parameters, developers can control IoT devices like actuators or motors through the gateway component.

The Consortium

OÉ Gaillimh NUI Galway — Project Coordinator

UBITECH ubiquitous solutions

cnit

berlin

aditess
Advanced Integrated Technology Solutions & Services

WINGS ICT Solutions

SINTEF

GRUPPO Maggioli

Univerza v Ljubljani

A Novel Reconfigurable by design Highly Distributed Applications Development Paradigm over Programmable Infrastructure

ARCADIA

www.arcadia-framework.eu

Edition 3

CONTACT

Dr. Adegboyega Ojo (Project Coordinator),
Insight Centre for Data Analytics, National University of Ireland (NUIG),
phone: +353 91 495336
email : adegboyega.ojor@insight-centre.org

Dr. Panagiotis Gouvas (Technical Coordinator),
UBITECH Ltd,
phone: +30 216 5000500
Email: pgouvas@ubitech.eu

PROJECT DETAILS

Start date: 01/01/2015
Duration: 36months
Reference: GA no 645372
Budget: 3,543,864 €
Funding: 3,543,864 €

www

This project has received funding from the European Union's HORIZON 2020 Programme, (Call H2020-ICT-2014-1), Grant no.645372

In **ARCADIA**, three use cases with four applications are developed and evaluated targeting different important areas:

i) **energy efficiency** and **QoS** trade off
ii) high performance survivable communications in **distributed IoT** deployments
ii) security and privacy support in the **FIWARE** platform

Energy Efficiency vs Quality of Service (QoS) trade-off

The transition to more energy efficient infrastructures has to take into account the implications to Quality of Service (QoS) / Quality of Experience (QoE) requirements based on the supported services and applications as well as the requirements imposed by the network administrators and services providers. Higher flexibility, enhanced control and management capabilities, are required to effectively deal with the performance/ power consumption trade-off, once the new dimension of energy-awareness is taken into account in all phases of network design and operation.

This challenge is going to be addressed based on the technological artefacts that will be developed within ARCADIA. Sophisticated distributed control/management techniques can be realistically deployed – both at the network edge and inside the network – to dynamically shape the allocation of resources and relocate applications and network functionalities, trading off QoS/QoE and energy at multiple granularity levels.

High Performance Survivable Communications in Distributed IoT Deployments Use Case

The High Performance Survivable Communications in Distributed IoT Deployments Use Case is based on the implementation of the 6inACTION PPDR technology (www.6inaction.net). 6inACTION is an advanced system designed to provide public safety agencies with a survivable, scalable and robust communications and professional IoT-supported intervention management services during day-to-day operation and disaster relief missions.

High-performance communications in day-to-day operations and survivable communications in extreme conditions have to be supported since the provided application is executed in a distributed system with distributed service intelligence. The innovation that will be added in 6inAction based on the implementation within ARCADIA regards the use of the project's technologies (especially the use of Smart Controller implementation in companion with OpenFlow technologies) for virtual channel establishment allowing for transparent communication via one or several available networks represented as a single virtual channel. Context-driven routing with dynamic QoS support and dynamic cross-network admission control and service pre-emption will be supported, while based on the provided implementation, very high availability with near-real-time reroute capabilities allowing for (almost) instant fall-back scenarios in case of extreme conditions causing failure of individual networks information driven servicing will be supported.

Security and Privacy Support in the FI-WARE Platform

FI-WARE (www.fi-ware.org) is an innovative, open cloud-based infrastructure for cost-effective creation and delivery of Future Internet applications and services, at a scale not seen before. FI-STAR (Future Internet Social and Technological Alignment Research) is a project that is an instantiation of the FI-WARE platform and aims to establish early trials in the Health Care domain building on Future Internet (FI) technology. The FI-STAR Platform services provide application modules, re-usable generic and health care sector specific functionality. The TUB FI-STAR Service Delivery Platform (SDP) is going to be used for the realization of the Security and Privacy Support in the FI-WARE Platform Use Case.

"Remote Patient Monitoring" is one of two applications selected to implement in the Security and Privacy Use Case to evaluate the capability and practical usability of ARCADIA framework towards supporting security and privacy requirements when developing and operating cloud applications. The RPM development follows the current FIWARE reference architecture to support developing IoT applications.