



NGI_TRUST 3rd Open Call (Ref: NGI_TRUST 2019003)

Call for proposals from the Partnership for innovative technological solutions to ensure privacy and enhance trust for the human-centric Internet – NGI_TRUST

Acronym: IoTrust

Secure trust bootstrapping and peer-to-peer network connections in the Internet of Things

Date of submission: 05-04-2020

Logo of partners



Odin Solutions SL (ODINS) - Spain	
Digital Worx GmbH (DW) - Germany	

Table of Content

1	Overview of the proposal	4
1.1	The applicant(s)	4
1.2	Executive summary.....	4
1.3	Objectives and type of project.	4
2	Novelty and Innovation	5
2.1	Beyond the State-Of-The-Art & Main Innovations	5
2.2	Main Outcomes related to NGI-TRUST Call, Topics and Areas.....	5
2.3	Market Potential & Global dimension	6
2.4	Contributions to Human-Centric Internet	6
2.5	Stakeholders Engagement and Dissemination	6
2.6	Intellectual Property Rights (IPR) and Relevance to Societal, Environment and Gender	6
3	Expertise and resources.....	7
3.1	Overview of the project team.....	7
3.2	Access to required resources or knowledge.....	8
4	Project planning and budget.	9
4.1	Project activities and milestones	9
4.2	Value for money	11
5	Signature.....	13
6	Annexes:	14
6.1	Information about third-party applying for financial support.....	14
6.2	Legal entity form.....	16
6.3	Statement of overall turnover (only applicable to legal entities)	18
6.4	Declaration on honour on exclusion criteria and selection criteria (only applicable to lead partner)	20
6.5	CVs	22
6.6	References	37

Index of Tables

Table 1	Contact person.....	4
Table 2	Overview of the partners	4
Table 3	Type of project	4
Table 4	Proposed Team	7
Table 5	Gantt Chart of Workplan.....	10
Table 6	Milestones.....	10
Table 7	Person-Month per Organization	11
Table 8	Total budget.....	11
Table 9	Legal entity.....	14

1 Overview of the proposal

1.1 The applicant(s)

Table 1 Contact person

Contact Name	Antonio Skarmeta Gomez
Contact e-mail	skarmeta@odins.es
Contact phone	+34 868123395

Table 2 Overview of the partners

Partners	Partner organisation name	Country
1	Odin Solutions SL (ODINS)	Spain
2	Digital Worx GmbH (DW)	Germany

1.2 Executive summary

Internet-of-Things (IoT) enables advanced applications and new business opportunities in global sectors like Industry 4.0, Smart Cities, Precise Agriculture and othersⁱ. However, existing IoT products fail to provide human-centric and trustworthy applications covering security/privacy requirements specified in **international legal regulations** such as: (1) GDPRⁱⁱ for data privacy and the protection of personal data, (2) NIS Directiveⁱⁱⁱ for internetwork operations and (3) EU Regulation No 526/2013^{iv} from ENISA for electronic communications, infrastructure and services. Moreover, **international studies** like “Industrie 4.0 Readiness”^v reveal that end-users are not able to setup and maintain easily IoT networks in a secure and trustworthy manner.

To setup IoT networks, the first process is secure bootstrapping. This involves authentication, authorization and key management operations that are vital to control network resources and communications. Nevertheless, **traditional bootstrapping protocols^{vi} are not adapted to recent IoT networks^{vii viii}** (e.g. NB-IoT^{ix}, LoRa^x, Sigfox^{xi}, etc) formed by IoT devices with limitations in computing and networking capacities to implement complex security protocols. Moreover, to maintain IoT networks it is required open and trustworthy solutions for detecting vulnerabilities in IoT software/hardware and providing robust update/patching management. However to maintain IoT networks, **current solutions^{xii xiii xiv} are complex, closed and non-interoperable** what do not permit the end-users to manage their networks with heterogeneous IoT devices in an easy and homogeneous way.

To tackle these challenges, IoTrust will implement and validate a **trustworthy, open and human-centric solution to setup and maintain IoT networks** based on the development and integration of a novel bootstrapping protocol, Peer-to-Peer and Distributed Ledger technologies in order to provide secure initialization of IoT devices, vulnerabilities detections and software patching/reprogramming. The proposed solution is based on recent standardization and research activities such as “**Secure IoT Bootstrapping**” draft^{xv} of IETF (Internet Engineering Task Force) and **Peer-to-Peer InterPlanetary File System (IPFS)^{xvi} with Distributed Ledger Technology to ensure decentralized IoT networks**. The main expected outcome will be a standards-based solution with open-source stacks for IoT devices and distributed services platform that will be **supported by real-world pilot validation**.

1.3 Objectives and type of project.

- **[O1]** Design a human-centric and open IoTrust solution to increase the user trust and application of secure IoT networks in worldwide sectors like Smart Cities, Industry 4.0, etc. **[Measurable (D1)]**;
- **[O2]** Develop and integrate novel bootstrapping, peer-to-peer and distributed ledger technologies to achieve trustworthy IoT networks and keep decentralized Internet infrastructure. **[Measurable (D2)]**;
- **[O3]** Validate technical features, key performance indicators and cyber-attacks protections of the IoTrust minimum viable product (MVP) using laboratory testbed and real-world pilots. **[Measurable (D3)]**;
- **[O4]** Perform dissemination activities and joint exploitation plan by making the most of real-pilot show-casting and coaching/mentoring process in order to foster valuable stakeholder engagement and the successful exploitation/commercialization of the results beyond the project **[Measurable (D4)]**.

Table 3 Type of project

Type of project/maximum funding	Type requested
Type 2 (execution): up to €150,000 from NGI_Trust, matching funds up to €75,000 (2/3 - 1/3 model).	X

2 Novelty and Innovation

The IoTrust aim is to provide simple setup and reliable operation of IoT networks in a trusted and secure manner automated setup of IoT peer-to-peer networks and open source stacks for worldwide applications.

To tackle the abovementioned challenges and satisfy the defined objectives, **IoTrust approach** is based on novel bootstrapping protocol, Peer-to-Peer and Distributed Ledger technologies in order to provide secure initialization of IoT devices, robust vulnerabilities monitoring and privacy-enhanced reprogramming.

IoTrust will provide a novel bootstrapping protocol, peer-to-peer network and distributed ledger system so setup IoT networks based on a dynamic calculated and secure trust score. IoT Devices, as participants in such dynamic networks can decide the level of interaction based on a calculated trust score.

In particular, the IoTrust solution will integrate an **innovative bootstrapping protocol called Low-Overhead CoAP-EAP (LO-CoAP-EAP)^{xvii} and based on three Internet standards:** Authentication, Authorization and Accounting (AAA) infrastructure^{xviii}, Extensible Authentication Protocol (EAP)^{xix} and Constrained Application Protocol (CoAP)^{xx}. First, AAA infrastructure enables scalability and roaming for the network access authentication. Second, EAP allows different IoT devices and organizations to use different authentication mechanisms (based on symmetric keys, certificates, etc.) depending on their requirements. Third, CoAP is an application protocol for IoT that enables Machine-to-Machine (M2M) communications. By building with these standardized protocols, LO-CoAP-EAP enables secure bootstrapping of distributed IoT networks to maintain a decentralized Internet infrastructure for the authentication and establishment of trustworthy, privacy and security between IoT devices and end-users services platforms. Integrating LO-CoAP-EAP, IoTrust provides a trade-off between **flexibility, networking technology independence, scalability and computing performance to enable trusted bootstrapping** of IoT devices to be deployed easily by any human without advanced computer knowledge.

Moreover, the IoTrust solution will incorporate a **novel dynamic trust scoring calculation and distribution method based on Peer-to-Peer InterPlanetary File System (IPFS) with Distributed Ledger Technology (DLT)** for automated connection and assessment of the trust level of IoT devices and their data. For human-centric management, this solution will also provide a distributed services platform where the registered IoT devices can be monitored (e.g. current trust level). To provide a high resilience, the IoT device information needed to calculate trust scores will be provided by homomorphic encryption in a distributed ledger.

2.1 Beyond the State-Of-The-Art & Main Innovations

To setup and maintain IoT networks, existing solutions^{xxi xxii xxiii} are mainly focused on closed non-interoperable software for exclusive hardware. Those solutions require specialized “know-how” for end users and operate on centralized services in private server making them vulnerable on cyber-attacks (e.g. DDoS). Current solutions do not support secure, trusted, open, sustainable and common management of heterogeneous infrastructure (e.g. IoT devices from different vendors). Beyond state-of-art, **the main innovations of IoTrust are:**

1. **Secure Bootstrapping of LO-CoAP-EAP** built with Internet standards for secure setup of IoT devices. (TRL4)
2. **Trust Monitoring:** Human-centric trust report of IoT devices to simplify the maintenance decisions making of inexperienced end-users for achieving cost effective and sustainable IoT infrastructure. (TRL5)
3. **Decentralized Peer-to-Peer Reprogramming:** High resilience against DDoS attacks by decentralized distribution of encrypted firmware, configurations and patches based on peer-to-peer IPFS networks. (TRL4)
4. **Trusted layer for IoT Networks:** DTL-based privacy-enhanced storage and IDs management to identify IoT devices and calculate their trust scores. (TRL5)

The IoTrust project is focused on the integration of these 4 main innovations developed currently in TRL4-5 to develop a human-centric and trusted solution that will be validated in real-world pilot scenarios (TRL 7).

2.2 Main Outcomes related to NGI-TRUST Call, Topics and Areas

The IoTrust outcomes will tackle two of four technological topics and three interest NGI-TRUST areas.

Areas of NGI-TRUST call	Realistic and measurable outcomes of IoTrust
Vulnerabilities in software/hardware.	IoTrust will extend and provide a platform to measure the trust level of IoT Devices and their Data (e.g. risk monitoring based on Peer-to-Peer IPFS and DTL technologies).
New protocols to bootstrap security and trust for end users and devices.	IoTrust will integrate and deliver a novel bootstrapping technology called LO-COAP-EAP for IoT devices and end-users platforms and the

	dynamic calculation of Trust Scores.
Open crypto software and hardware that can be used by users.	IoTrust will distribute open source IoT stack integrated with crypto mechanisms (e.g. EAP, DLT, etc) and standardized protocols (e.g. COAP, IPFS) in a public Internet repository (e.g. Github ^{xxiv})

The IoTrust outcomes will enable **high applicability** for trusted operation of large scale IoT infrastructure in connected smart environments such as city, industry, agriculture, etc. Beyond the project, these **open outcomes** could be reused by Internet developers' communities (e.g. Arduino^{xxv}, ContikiOS^{xxvi}, Linux^{xxvii}, etc).

2.3 Market Potential & Global dimension

Global Market for Internet of Things (IoT) is rising from **25 Billion devices in 2018 to more than 125 Billion devices in 2025**. And the global IoT market will reach USD1.567 Trillion by 2025 (forecasts of Forbes^{xxviii}). The IoT networks are fundamental for novel services and applications in almost all markets such as industry 4.0, smart cities, precise agriculture, autonomous vehicles, smart energy, etc. Furthermore, global activities are in progress to foster vendors and users towards IoT products with high security/trustworthy by standardization efforts and regulations (e.g. ENISA and EU Cybersecurity Act^{xxix}). Cybercriminals have already discovered the potential of exploiting vulnerabilities of IoT devices as tools for operating botnet and malware distribution (e.g. 2016 Mirai botnet^{xxx}). Therefore, IoTrust **is targeting this strong growing market** by offering standards-based bootstrapping and distributed ledgers technologies for trusted secure setup and trusted maintenance of IoT devices for their lifetime.

2.4 Contributions to Human-Centric Internet

Nowadays, IoT solutions are still too device-centric based on monitoring and control systems from private vendors without considering the human needs^{xxxi}. **To contribute to more human-centric Internet**, IoTrust will provide secure bootstrapping and trusted vulnerabilities management that require minimal human interaction and facilitate the maintenance decision making. Therefore, IoTrust will make IoT networks more trustworthy for maintenance operators, resilient against cybercriminals and inclusive to end-users without computer knowledge. Moreover, IoTrust solution is based on **open stacks and standardized protocols** to allow more sustainable maintenance of IoT networks without vendors' dependency. Additionally, IoTrust will be followed a SCRUM methodology of iterative cycles for design/development/validation in **close cooperation with end-users and stakeholders** in order to improve the solution in a more human-centric manner.

2.5 Stakeholders Engagement and Dissemination

IoTrust is founded with a multi-actors strategy and has already the support of key end-users of multiple sectors. This ensures early engagement and continuous inputs since the beginning of the project. Furthermore, the consortium will employ **open source repositories** (e.g. Github) and **open management tools** (e.g. Trello^{xxxii}) **to share the periodic advances** in order to foster the active participation of stakeholders like Internet developers community. Moreover, the consortium will prepare **communication material** (e.g. flyer, presentation, poster, roll-up, scientific publication, video) and will perform **dissemination activities in international events and communication channels** such as:

- Email marketing and social networks (e.g. Mailchimp, Twitter, Linkedin, Facebook, Youtube).
- Congress/workshops of IoT and Open-Source (e.g. IoT Solutions World Congress, OpenSource Workshop).
- Trade events or market fairs of SmartCities, Industry 4.0, Agriculture (e.g. VDMA, Allianz Industrie 4.0).
- Scientific conferences or journals related to Next Generation Internet and Security/Privacy/Trust in IoT.

2.6 Intellectual Property Rights (IPR) and Relevance to Societal, Environment and Gender

The IoTrust stack for IoT devices will be developed as **Open Source (e.g. Apache 2.0 license)** to spread this use as wide as possible. IoTrust will allow that vendors and operators of IoT devices can include the open-source libraries to implement secure bootstrapping and privacy vulnerabilities management in their IoT networks. The use of IoTrust Open Source libraries will enable them to reduce their own costs on developing such solutions out of the scratch. Moreover, the **Open-Source Peer-Review Process** will increase the security and sustainability of IoTrust solution compared to proprietary solutions. The IoTrust libraries will be openness to any human without limitations of gender, race or nationality. Furthermore, the IoTrust firmware updates will increase the lifetime of IoT devices in order **to minimize electronic waste and environment pollution**.

3 Expertise and resources

3.1 Overview of the project team

Thelo Trust consortium consists of a **transnational and multi-disciplinary team**. The consortium has the **right balance of research/development skills, business scope and roles**, essential to achieve the indicated outcomes.

Table 4 Proposed Team

Name	Entity	Role in the project
Antonio Skarmeta	ODINS	Main Cybersecurity Researcher
Rafael Marin Perez	ODINS	Researcher & Developer in Internet of Things and Security/Privacy
Dan Garcia Carrillo	ODINS	Researcher & Developer in Secure IoT Stack
Mirko Ross	DW	Expert on Human-Centric Solution and Creative Exploitation Strategy
Silke Capo	DW	DTL Researcher in Distributed Platform and Human-Centric Services
Mihaly Virag	DW	DTL Architect of Distributed Platform and Human-Centric Services

3.1.1 Explain why the team is well placed to deliver the expected results. (Please, see more details in 6.5)

Dr. Antonio Skarmeta Gomez (CIO of OdinS). He received Ph.D. in Computer Science from the University of Murcia in 1995. He is professor from the University of Murcia since 1997. Moreover, he is cofounder and CIO of the spin-off OdinS since 2014. He has directed **31 doctoral theses**, participated in **more 25 European projects** and has coordinated several international projects (FP6, FP7, H2020). He has obtained **29 research contracts** with numerous regional, national and international companies and he has developed **9 patents and more 20 property registers**. He has published over **120 JCR papers with more 50 Q1 and more 200 papers** in international congresses. According to Google-Scholar, his publications have **11902 cites** and his **index-H is 45**. He has participated on **more 40 technical program committees** of the most relevant conferences in Computer Science, Security/Privacy and Internet of Things. He has been **associate editor of IEEE Trans SMC.Part B, Security and Communication Networks Magazine** and **more 10 special issues of JCRs**. Another indicator of his research contribution is the generation of technology knowledge transferred to Internet community (i.e. **OpenIKeV2**). He has participated in several standardization activities being co-authors of some drafts about security and communications at the **IETF, and participant of WG on ETSI (INS ING) and ISO WG**. **Antonio will participate actively on T.1 Design and T.3 Validation and will lead T.4 Dissemination & Exploitation.**

Rafael Marin Perez (Researcher in OdinS). He received his Ph.D. (Hons.) in Computer Science at University of Murcia in 2012. Since 2006, he has worked as full-time researcher on **more 10 international projects and more 8 national R&D projects** in the field of Wireless Sensor Networks, Internet of Things, Security/Privacy. The main quality indicators are the relevance of congresses and journals where their scientific-technological research has been published in the area of telecommunications and security (**8 JCR, 6 Q1, 6 int. congresses**). According to Google-Scholar, his publications have **525 cites and his index-H is 11**. In addition, he has collaborated in **8 Technical Program Committees (TPC) and 2 standardization groups** such as Irrigation systems within ISO and Context Information Management within ETSI. **Rafael will work actively on T.1 Design, T.2 Development and T.3 Validation so as T.4 Dissemination & Exploitation.**

Dan Garcia Carrillo (Researcher in OdinS). He received his Ph.D. in Computer Science at the University of Murcia in 2018 with the **thesis titled "A CoAP-Based Bootstrapping Service for Large-Scale Internet-of-Things Networks"**. Currently he is a postdoctoral researcher on security/privacy protocols to guarantee trusted IoT networks in different types of constrained networks such as 6LoWPAN, 6TiSCH, LPWAN and, recently 5G. He has collaborated in **4 European R&D projects (H2020, FP7)** in the areas of Internet of Things and Cybersecurity. His researches have been published in **4 international congresses, 7 JCR with 4 first quartiles (Q1)**. Moreover, he has contributed to **5 standardization drafts in the IETF and has 1 property register** regarding security and bootstrapping for decentralized Internet infrastructure. He was **TPC of SPIoT 2018**. **Dan will lead T.2 Development and will work actively on T.1 Design and T.3 Validation.**

Mirko Ross (CEO of DW). In 1998 he graduated at University of Applied Science Nürtingen with excellence. Since 1998 he has **founded 3 companies in the ICT sector**. He has participated on more **30 R&D private contracts and 10 international/national R&D projects** achieving **8 international awards** in the area of security and IoT solutions. He is involved in public and private research activities for **human-centric solutions and disruptive business models**. He is technical **lead Advisor at Blackpin Secure Communication** and Member of the advisory board of DigitCode, a company focusing the improvement of reliable IoT communication. He is **Co-Chair of the AIOTI Working Group Distributed Ledger**. In the European Commission's Future Internet program he supported as a **business coach for startups in human-centric solutions** for eHealth and Industrial 4.0. Since

2016 he is coaching SME and Startups in the European SME Instrument. Since 2017 Mirko is a member of the **IoT Security Expert Group of the European Agency of Network and Information Security ENISA**. He is Member of the **IOTA Evangelist Network (IEN)** to support **Blockchain and Distributed Ledger** technologies. **Mirko will lead T.1 IoTrust Design and will work actively on T.3 Validation and T.4 Dissemination & Exploitation.**

Silke Capo is senior platform developer at DW. In 1998, she graduated at University of Applied Science Ludwigsburg. In 1999, she started working as software developer with focus on web-application and e-business. Since 2011 Silke is working as senior software developer and project consultant at digital worx, with a strong focus on innovation and human-centric solutions. During her professional career, she has participated on **more 20 R&D private contracts** and 7 international/national R&D projects achieving **7 international awards** in the areas of **Peer-to-Peer IPFS and Distributed Ledger technologies**. She is trained for **agile development and validation with SCRUM methodology** for software projects in DW company. **Silke will lead T.3 Validation and will work actively on T.1 Design and T.2 Development.**

Mihaly Virag is senior platform developer at DW. In 2003 he finished his studies of computer science at University Gabor Denes, Budapest. From 2002 to 2008, Mihaly was collaborated on research and development projects for Hungarian National Institute (NIVE) supported by the European Committee in the framework of Leonardo da Vinci cooperation program. Since 2011 he is working at DW as senior developer and active researcher and lead architect. He has worked on more **15 R&D private contracts** and 7 international/national R&D projects achieving **7 relevant awards** in the areas of **Peer-to-Peer IPFS and Distributed Ledger technologies**. **Mihaly will work actively on T.1 Design, T.2 Development and T.3 Validation.**

3.1.2 Have the team members/organisations worked together before?

DW and OdinS have successfully **collaborated in a H2020 project called IoTcrawler (Grant Agreement 779852)** to research several key enablers **to develop a secure search engine for decentralized internet infrastructure** of IoT networks and cloud platforms. In IoTcrawler, DW and OdinS have started the researches in secure bootstrapping and distributed ledger technologies. The outcomes of IoTcrawler project in **TRL4-5 will be extended in IoTrust including peer-to-peer reprogramming and vulnerabilities monitoring to develop an integrated MVP** of trustworthy setup and vulnerability maintenance that **will be validated in real-world pilots (TRL7)**. Moreover, IoTcrawler has performed a user-centric requirements analysis in global domains like SmartCities and Industry 4.0. This analysis will be considered in the human-centric design and development of the IoTrust solution.

3.2 Access to required resources or knowledge.

OdinS is a spin-off of University of Murcia (UMU) and works in close cooperation with UMU research groups in areas of IoT and cybersecurity. OdinS has **high-quality facilities for research and development** including electronic workspaces, computing laboratories, meeting rooms and networking spaces. Moreover, the spin-off has **an IoT testbed of devices and a data centre** for experimentations, services provision and processing simulations. OdinS provides wide expertise on R&D projects developing IoT devices and communication stacks compatible with standardized protocols and open cloud platforms like FIWARE. OdinS has participated on **ARMOUR H2020 FIRE project** for the research and development of IoT stacks of security-by-design and privacy-by-design communications. Moreover, OdinS has researched security components for IoT devices to support distributed access control (i.e. DCapBAC) and privacy preserving technique (i.e. CP-ABE) and **security bootstrapping (i.e. LO-COAP-EAP)**. Recently, OdinS has published "Security association establishment based on bootstrapping technologies for enabling secure IoT infrastructures. **JCR index 4.693 Future Generation Computer Systems** 95, 570-585 (2019)". Furthermore, OdinS participates actively on **standardization groups of ETSI and IETF about Security and Internet communications**. Currently, OdinS is working on an **IETF Draft about "Secure IoT Bootstrapping"**. (Please, see more details in section 6.5)

DW has expertise on developing and applying secure and human-centric IoT solutions in several industrial sectors like Industry 4.0 and Smart Agrifood. In particular, **DW has developed human-centric applications** for quality management, predictive maintenance, production workflow optimizing and mobile data visualisation. Moreover, **DW provides an industrial testbed in its Stuttgart location** and has IoT devices in experimentation and testing at the Future Work Lab at Fraunhofer IAO. **DW as initiator of the LoRa Things Network in Stuttgart** has deployed a large-scale testbed with over 30 LoRa Gateways covering IoT applications on a radius of 50km. The company has expertise on **KATANA H2020 project researching security layers on IoT platforms** to improve the food supply chain. Furthermore, DW has provided their experiences in **Distributed Ledger Technologies (DLT) in international organizations** like Dubai Future Foundation, Teqnocrats Tokyo DLT Hub and AIOTI Blockchain Working Group. In particular, DW is researching and developing **asvin.io platform**, a DLT-based trust system for remote management of IoT devices. Recently, DW has received a **Special Jury Award for asvin.io** at Tokio FIBC (Financial Innovation Business Conference). (Please, see more details in section 6.5)

4 Project planning and budget.

4.1 Project activities and milestones

4.1.1 Main activities of the sub-project.

IoTrust will be designed and developed following a human-centric and open-source method based on Agile SCRUM with “adaptive life cycles”. In the IoTrust project, each SCRUM sprint cycle will be 2 weeks, with a result review after and adjustment of development backlog for next sprint. By that, the project will be developed in a controlled iterative procedure. This method enables iterative cycles for design/development/validation to improve the solution with end-user interaction. It enables the continue end-users interaction to validate the development, so feedback from end users and stakeholders will be used to improve the design/development that is especially useful to engage the end-users and stakeholder participation. Moreover, **IoTrust emphasizes transparency, inspection and adaptation that are three critical pillars to the open source community^{xxxiii}**. To do that, IoTrust consortium will publish periodic advances in forums of Internet developing community using open source repositories (e.g. Github) and open management tools (e.g. Trello) to foster the engagement of end-users and stakeholders. The IoTrust method of software co-creation will **deliver a human-centric IoTrust MVP (Minimum Viable Product) for the transition to its commercialization beyond the project**. Following this approach, the **main activities** of IoTrust project will be:

- Designing a human-centric solution based on the needs of end-users and stakeholders like IoT developers.
- Developing and integrating a trusted solution based open source stacks and standardized protocols.
- MVP demo and validation of the IoTrust solution in real-world pilot scenarios.

To cover the main activities of the project and satisfy the objectives defined, the next **tasks (T)** are identified:

T.1 IoTrust Architecture Design -Duration: M1-M6 -Leader: DW -Objective: O1

Approach: T.1 will design a human-centric architecture solution according to the requirements of end-users and other stakeholders like Internet developers. To do that, this task will take the most of the user-centric requirement analysis defined in IoTcrawler project as well as the active participation of supported end-users. Moreover, T.1 will tackle critical aspects like users interaction and open source sharing. This task will define SCRUM software backlog, end-users interfaces, APIs and open-source libraries so as validation factors for T.3.

Roles: DW will be in charge of the design with the support of OdinS for IoT stack.

T.2 Open Standards-based IoTrust Development -Duration: M2-M8 -Leader: OdinS/DW -Objective: O2

Approach: T.2 will follow the design of T.1 to develop a trusted solution integrated bootstrapping technique (i.e. LO-COAP-EAP) and vulnerabilities management suite (i.e. asvin.io) based on standardized Internet protocols (i.e. COAP, EAP, IFPS and Blockchain) and open source stacks (e.g. Arduino, ContikiOS, Linux). This development will be performed in iterative development cycles considering the end-users/stakeholders feedback and validation performed in the task T.3.

Roles: OdinS will develop software elements of IoT devices and DW will extend software of cloud platform.

T.3 MVP Demo and Pilot Validation -Duration: M3-M9 -Leader: OdinS -Objective: O3

Approach: T.3 will validate and evaluate the developed MVPs of T.2 according to the factors defined in T.1 for human-centric features, open-source aspects, security/privacy protections and key performance indicators. This task will validate the MVP development in testbed laboratories of OdinS (Spain) and DW (Germany) as well as in two real-world pilots: Smart City of Murcia (Spain), and Industry Monitoring Applications (Germany). This task will provide the validation results and the end-users & stakeholders opinions to feed the tasks of T.1 design and T.2 development. The result of this task will be a MVP product (TRL7) of the human-centric IoTrust solution evaluated in real-world pilots in operational environments.

Roles: OdinS will coordinate this task. Both OdinS and DW will be in charge of validations in their countries.

T.4 Dissemination and Exploitation -Duration:M3-M9 -Leader: DW/OdinS -Objective: O4

Approach: T.4 focuses on the preparation and execution of all activities related to outcomes dissemination, stakeholder engagement and joint exploitation strategies. This task will disseminate the project results obtained in the technical tasks (T.1, T.2 and T.3). Dissemination will attend to global audiences (e.g. Internet Community, IoT providers, Open Source developers, Security experts, etc) that may show interest in the results of the project. To do that, this task will make the most of real-pilots show-casting and NGI coaching/mentoring process to foster the engagement of end-users. For the exploitation of IoTrust MVP, both OdinS and DW will define a joint strategy plan with Business Model Canvas. OdinS and DW will address two main models of exploitation of

the IoTrust results: 1) Commercial exploitation model that involves the sale of in product or service format to end users, complying with a scheme that will be defined in the business model, 2) Model of research exploitation that implies the reuse of the acquired knowledge (Know-How) in future R&D projects in international cooperation.

Roles: Both OdinS/DW will participate actively on this task to maximize the project impact.

To monitor and report the mentioned tasks, the following **deliverables (D)** will be provided:

D1. IoTrust Architecture Design (M6, DW): will report the IoTrust architecture design considering the needs of end-users and Internet developers so as critical aspects such as user interfaces, APIs, open source sharing and validation factors. This design will be updated during the iterative cycles of development and validation.

D2. Open Standards-based IoTrust Development (M8, OdinS) will describe the IoTrust prototype implemented of functional blocks, open source stacks and cloud services to enable setup and maintenance of IoT networks.

D3. MVP Testbed & Pilot Validation (M9, DW) will provide the IoTrust MVP solution with all components installed and validated in laboratories and real-world pilots.

D4. Dissemination and Exploitation (M9, OdinS/DW): will describe the dissemination activities performed and the defined plan for the exploitation strategies of IoTrust results regarding commercial and research models.

4.1.2 Work-plan and milestones

The following tables present the **work-plan** of the previous interrelated tasks and the **milestones (MS)** identified.

Table 5 Gantt Chart of Workplan

Task/Month	M01	M02	M03	M04	M05	M06	M07	M08	M09
T.1 IoTrust Architecture Design						D1			
T.2 Open Standards-based Development								D2	
T.3 MVP Demo and Pilot Validation									D3
T.4 Dissemination & Exploitation									D4
Milestones	MS1					MS2		MS3	MS4-5

Table 6 Milestones

Nº	Milestone description	Task	Deadline
MS1	Designed initial version of IoTrust architecture	T.1	M1
MS2	Enhanced final version of IoTrust architecture	T.1	M6
MS3	Implemented final prototype with all components integrated	T.2	M8
MS4	Validated Minimum Viable Product (MVP) in real-world pilots	T.3	M9
MS5	Done dissemination activities and IoTrust exploitation plan	T.4	M9

4.2 Value for money

Table 7 indicates the number of person-months (full-time equivalent) of people involved in the sub-project. The most PMs are dedicated to the needed effort for the technical tasks of design T.1, development T.2 and validation T.3.

Table 7 Person-Month per Organization

Name	Organisation	Person months
Antonio Skarmeta Gomez	ODINS	5
Rafael Marin-Perez	ODINS	7
Dan Garcia Carrillo	ODINS	8
Mirko Ross	Digital Worx	4
Silke Capo	Digital Worx	6
Mihaly Virag	Digital Worx	5
TOTAL		36

In Table 8, the total budget is presented with the personnel costs, equipment costs and travel expenses. There is not cost of software licenses, because the IoTrust project is based on open source. Due to the type 2 of the project requested, each partner will contribute with its own funds to the 1/3 part of the total budget. OdinS and DW can ensure these own funds, because their annual business benefits are higher than these specified funds.

Table 8 Total budget

Item	OdinS	Digital Worx	Total
Personnel costs	102900	112500	215400
Equipment costs*	0	0	2900
Software licenses*	0	0	0
Travel expenses*	2800	2100	2000
Total Costs	105700	114600	220300
Requested contribution** 2/3	70466,66667	76400	146866,66667
Own Funds ** 1/3	35233,33333	38200	73433,33333

* In as much as they are required for the execution of the project

** Type 2 (execution): up to €150,000 from NGI_Trust -> matching funds up to €75,000 (2/3 - 1/3 model);

Below, each partner provides further details and explanations about the funding requested.

Justification of OdinS costs

1) Personnel costs of 20 Person Months (102900 Euros) to perform the following tasks:

- Participating actively in the task T.1 to design the human-centric IoTrust solution in the part of open stack for IoT devices.
- Working actively on the task T.2 to develop the open standards-based stack for IoT devices and support the integration with IoTrust services platform which will be reported in the deliverable D.2.
- Leading the task T.3 to validate and refine the IoTrust solution in laboratory testbed and pilot scenarios which will be described in the deliverable D.3.
- Collaborating to the task T.4 to perform the international activities of dissemination, stakeholder engagement and exploitation definition that will be reported in the deliverable D.4.

2) Travel expenses: 2.800 Euros

- Local trips for deployment and validation at pilot scenario of Smart City in Murcia.

- 3 Dissemination events (one for each phase, 500€ per trip for 1 personnel).
- 2 NGI-TRUST meetings to attend coaching and mentoring activities (500€ per business trip for 1 personnel).

Justification of Digital Worx costs

1) Personnel costs of 15 Person Months (112.500 Euros) to perform the following tasks:

- Leading the task T.2 to design the human-centric IoTrust solution in the parts of open IoT stack and distributed services platform which will be reported in the deliverable D.1 including SCRUM software backlog, end-users interfaces, open-source libraries and validation factors.
- Collaborating to the task T.2 to develop the IoTrust services platform and support the implementation of open IoT stack.
- Participating actively in the task T.3 to deploy, validate and refine the distributed services platform in laboratory testbed and real pilots.
- Collaborating to the task T.4 to perform the international activities of dissemination, stakeholder engagement and exploitation definition that will be reported in the deliverable D.4.

2) Travel expenses: 2.100 Euros

- Local trips for deployment and validation at industrial pilot scenario in Stuttgart.
- 2 Dissemination events (one for each phase, 500€ per trip for 1 personnel)
- 2 NGI-TRUST meetings to attend coaching and mentoring activities (500€ per business trip for 1 personnel).

5 Signature

The application form may be digitally signed.

Lead Partner

Name of signatory

Jose Trigueros Pacheco

Place, Date

Murcia, Spain, 01 May 2020

Signature



6 Annexes:

6.1 Information about third-party applying for financial support

Table 9 Legal entity

Lead Partner	
Legal Name	Odin Solutions SL
Type of legal entity	SME
PIC number*	934796858
VAT registration number*	ESB73845893
Business register number*	ESB73845893
Business register location*	Murcia (Spain)
Country	Spain
Legal Address	C/ Perú, 5, 3º, Oficina 12, Polígono Industrial Oeste, 30820 Alcantarilla (Murcia)
Name of legal signatory	Jose Trigueros Pacheco
Type of Activity	ICT Provider of IoT devices and platforms
Business sector	Industry 4.0, Smart Cities and Precise Agriculture
Have you received funding from the Horizon 2020 project before? (Yes/No) If yes please indicate the Grant Agreement number(s)	Fed4IoT (GA-814918), Plug-n-Harvest (GA-768735), ANASTACIA (GA-731558), IoT-Crawler (GA-779852), Cpaas.io (GA-723076) and ARMOUR (GA-688237).
Have you received funding from NGI project(s) (as a legal entity) or worked on NGI-funded project(s) (as an individual) before? (Yes/No) If yes, please indicate the NGI project(s)	No
Have you received other EU funding (as legal entity) or worked on EU-funded project(s) (as individual) related to this proposal? (Yes/No) If yes, please indicate from which programme(s)	No


**if applicable*

Partner 2	
Legal Name	Digital Worx GmbH
Type of legal entity	SME
PIC number*	941561735
VAT registration number*	DE218401190
Business register number*	HRB: 225281
Business register location*	Amtsgericht Stuttgart
Country	Germany
Legal Address	Schulze-Delitzsch-Str. 16, 70565 Stuttgart, Germany
Name of legal signatory	Mirko Ross
Type of Activity	ICT Solution provider
Business sector	Industry 4.0, IIoT, IoT
Have you received funding from the Horizon 2020 project before? (Yes/No) If yes please indicate the Grant Agreement number(s)	KATANA (GA- 691478) and IoTcrawler (GA-779852).
Have you received funding from NGI project(s) (as a legal entity) or worked on NGI-funded project(s) (as an individual) before? (Yes/No) If yes, please indicate the NGI project(s)	No
Have you received other EU funding (as legal entity) or worked on EU-funded project(s) (as individual) related to this proposal? (Yes/No) If yes, please indicate from which programme(s)	No

**if applicable*

6.2 Legal entity form

Legal entity form of Odin Solutions SL.



PLEASE COMPLETE AND SIGN THIS FORM AND ATTACH COPIES OF OFFICIAL SUPPORTING DOCUMENTS (REGISTER(S) OF COMPANIES, OFFICIAL GAZETTE, VAT REGISTRATION, ETC.)

LEGAL ENTITY

PRIVACY STATEMENT http://ec.europa.eu/budget/library/contracts_grants/info_contracts/privacy_statement_en.pdf


Please use CAPITAL LETTERS and LATIN CHARACTERS when filling in the form.

PRIVATE LAW BODY


OFFICIAL NAME ①	ODIN SOLUTIONS, S.L.		
BUSINESS NAME (if different)			
ABBREVIATION	ODINS		
LEGAL FORM	SOCIEDAD LIMITADA		
ORGANISATION TYPE	FOR PROFIT <input checked="" type="checkbox"/>		
	NON FOR PROFIT <input type="checkbox"/>	NGO ② YES <input type="checkbox"/> NO <input type="checkbox"/>	
MAIN REGISTRATION NUMBER ③	REGISTRO MERCANTIL DE MURCIA, TOMO 3055, LIBRO 0, FOLIO 11, HOJA MU-8635		
SECONDARY REGISTRATION NUMBER (if applicable)			
PLACE OF MAIN REGISTRATION	CITY	MURCIA	
	COUNTRY	ESPAÑA	
DATE OF MAIN REGISTRATION	13	06	2014
	DD	MM	YYYY
VAT NUMBER	ESB73845893		
ADDRESS OF HEAD OFFICE	POLIGONO INDUSTRIAL OESTE, CIPERU, S. 3º, OFICINA 12		
POSTCODE	30820	P.O. BOX	
		CITY	ALCANTARILLA (MURCIA)
COUNTRY	ESPAÑA	PHONE	+34 868 123395
E-MAIL	INFO@ODINS.ES		

DATE 17/04/2019

SIGNATURE OF AUTHORISED REPRESENTATIVE



STAMP




① National denomination and its translation in EN or FR if existing.

② NGO = Non Governmental Organisation, to be completed if NFPO is indicated.

③ Registration number in the national register of companies. See table with corresponding field denomination by country.

Legal entity form of Digital Worx GmbH.



PLEASE COMPLETE AND SIGN THIS FORM AND ATTACH COPIES OF OFFICIAL SUPPORTING DOCUMENTS (REGISTER(S) OF COMPANIES, OFFICIAL GAZETTE, VAT REGISTRATION, ETC.)

LEGAL ENTITY


PRIVACY STATEMENT http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm#en

Please use CAPITAL LETTERS and LATIN CHARACTERS when filling in the form.


PRIVATE/PUBLIC LAW BODY WITH LEGAL FORM

OFFICIAL NAME ①	digital worx GmbH		
BUSINESS NAME (if different)			
ABBREVIATION			
LEGAL FORM	GmbH		
ORGANISATION TYPE	FOR PROFIT	<input checked="" type="checkbox"/>	
	NON FOR PROFIT	<input type="checkbox"/>	NGO ② YES <input type="checkbox"/> NO <input type="checkbox"/>
MAIN REGISTRATION NUMBER ③	225281		
SECONDARY REGISTRATION NUMBER (if applicable)			
PLACE OF MAIN REGISTRATION	CITY	Stuttgart	
	COUNTRY	Germany	
DATE OF MAIN REGISTRATION	14	09	2001
	DD	MM	YYYY
VAT NUMBER	DE218401190		
ADDRESS OF HEAD OFFICE	Schulze-Delitzsch-Str. 16		
POSTCODE	70565	P.O. BOX	
		CITY	Stuttgart
COUNTRY	Germany	PHONE	0049 711 22040930
E-MAIL	info@digital-worx.de		

DATE 26/03/2016

SIGNATURE OF AUTHORISED REPRESENTATIVE


STAMP



① National denomination and its translation in EN or FR if existing.

② NGO = Non Governmental Organisation, to be completed if NFPO is indicated.

③ Registration number in the national register of companies. See table with corresponding field denomination by country.

6.3 Statement of overall turnover (only applicable to legal entities)

The undersigned, Jose Trigueros Pacheco, hereby provides a statement of overall turnover for the last 2 financial years and declare that the following financial figures are truthful for Odin Solutions SL:

	FY 2017	FY 2018
Overall turnover	192.247,42€	231.628,55€

Signed in Murcia on 29 April 2019

Name: Jose Trigueros Pacheco

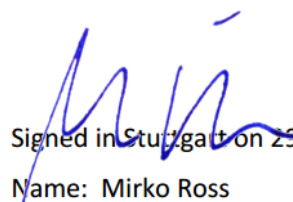
Function: CEO

Company: Odin Solutions SL



The undersigned, [Mirko Ross], hereby provides a statement of overall turnover for the last 2 financial years and declare that the following financial figures are truthful for [Digital Worx GmbH]:

	FY 2017	FY 2018
Overall turnover	€800.00	€850.000



Signed in Stuttgart on 29 April 2019

Name: Mirko Ross


Function: CEO

Company: Digital Worx GmbH

6.4 Declaration on honour on exclusion criteria and selection criteria (only applicable to lead partner)

The undersigned Jose Trigueros Pacheco, representing:

ID or passport number: 52800781-A ('the person')	Full official name: Jose Trigueros Pacheco Official legal form: CEO of Odin Solutions SL Statutory registration number: Registro Mercantil de Murcia, Tomo 3055, Libro 0, Folio 11, Hoja MU-86357, Inscripción 1ª Full official address: C/ Perú, 5, 3º, Oficina 12, Polígono Industrial Oeste, 30820 Alcantarilla (Murcia) VAT registration number: ESB73845893
--	--



('the person')

1. Declares that is not in one of the following situations:

- a) it is bankrupt or being wound up, is having its affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, is the subject of proceedings concerning those matters, or is in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- b) it or persons having powers of representation, decision making or control over it have been convicted of an offence concerning their professional conduct by a judgment which has the force of res judicata;
- c) it has been guilty of grave professional misconduct proven by any means which the contracting authority can justify including by decisions of the European Investment Bank and international organisations;
- d) it is not in compliance with its obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed;
- e) it or persons having powers of representation, decision making or control over it have been the subject of a judgment which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity, where such illegal activity is detrimental to the Union's financial interests;
- f) is subject to an administrative penalty for being guilty of misrepresenting the information required by the contracting authority as a condition of participation in a grant award procedure or another procurement procedure or failing to supply this information or having been declared to be in serious breach of its obligations under contracts or grants covered by the Union's budget.

2. Declares that:

- a) is not subject to a conflict of interest;
- b) has not made false declarations in supplying the information required by the as a condition of participation in the Open Calls of NGI_TRUST Project or does not fail to supply this information;
- c) is not in one of the situations of exclusion, referred to in the abovementioned points a) to f).
- d) Is aware and fully accepts all NGI condition and rules as expressed in NGI_TRUST open call Guide for Applicants.

3. Certifies that:

- is committed to participate in the abovementioned project;
- has stable and sufficient sources of funding to maintain its activity throughout its participation in the above-mentioned project and to provide any counterpart funding necessary;
- has or will have the necessary resources as and when needed to carry out its involvement in the above-mentioned project;
- no Consortium partner has received an amount greater or equal to €200.000 in total (including this proposal) via open calls of NGI projects.

4. Supporting documents (on request)

For situations described in point 1 (b), (c) or (e), production of a recent extract from the judicial record is required or, failing that, an equivalent document recently issued by a judicial or administrative authority in the country of establishment of the person showing that those requirements are satisfied.

For the situation described in point 1 (a), (d) or (f), production of recent certificates issued by the competent authorities of the State concerned are required. These documents must provide evidence covering all taxes and social security contributions for which the person is liable, including for example, VAT, income tax (natural persons only), company tax (legal persons only) and social security contributions. Where any document described above is not issued in the country concerned, it may be replaced by a sworn statement made before a judicial authority or notary or, failing that, a solemn statement made before an administrative authority or a qualified professional body in its country of establishment.

Full name: Jose Trigueros Pacheco

Date: 01-05-2020

Signature

A handwritten signature in blue ink, appearing to read 'Trigueros', is written over a green circular stamp. The stamp contains the word 'Odin' in a stylized font, followed by a large letter 'S' inside a circle.

6.5 CVs

Part A. Personal Data

Name	Antonio F. Skarmeta Gómez		
DNI/NIE/Passport	28710458H	Years	56
Id of researcher	ResearcherGate	https://www.researchgate.net/profile/Antonio_Skarmeta	
	Orcid Code	https://orcid.org/0000-0002-5525-1259	

A.1. Current Professional Situation

Entity	Odin Solutions SL		
Department	Research and Innovation		
Address	Calle Perú 5, Piso 3, Ofician 5, 30850, Alcantarilla, Pol. Oeste, Murcia		
Phone	+34 868123395	Email	skarmeta@odins.es
Position	Chief Innovation Officer (CIO)	Start Date	1/10/2014

A.2. Academic Education

Degree in computer science	University of Granada, Spain	1991
PhD in computer science	University of Murcia, Spain	1995
Professor in computer science	University of Murcia, Spain	1997

A.3. General KPI of the quality of scientific production

Total cites: 11902 (according to Google Scholar)	Number of patents: 9
Total JCR publications in first quartile (Q1): 51	Number of property registers: 21
Index h: 45 (according to Google Scholar).	Number of JCR publications: > 120
Number of R&D international projects: >25	Number of int. congress: > 200
Number of research contracts: 29	Member of Technical Program Committee: >40
Number of doctoral theses directed: 31	Co-editor of special issues: >10

CV Summary:

Antonio Skarmeta was born in Santiago de Chile in April 1965, obtaining a degree in Computer Science from the University of Granada in 1991 and a Doctorate in Computer Science from the University of Murcia in 1995. He is professor from the University of Murcia since 1997. Moreover, he is cofounder and CIO of the spin-off OdinS since 2014. He has been the **national representative of MINECO in the H2020 program** for the pillar of Excellent Science in the area of **MARIE SKLODOWSKA-CURIE**, as well as representative in the Human Resources and mobility group of the European Commission. He has directed 31 doctoral theses, participated in more 20 European projects and has coordinated several international projects including H2020, Regions of Knowledge, TEMPUS and Research Potential. He has obtained 29 research contracts with numerous regional, national and international companies and is the author of 9 patents and more 20 property registers. He is the author of more than 120 JCR publications in international journals, 200 articles in international congresses. He has participated on **technical program committees of the most relevant conferences in Computer Science, Security/Privacy and Internet of Things** such as Ad-hoc NoW, IEEE SMC, ACM Group, IEEE MSN, IEEE Globecom, IEEE TrustBus, etc. He has been member of the program committee of more than 40 peer-reviewed conferences. He has been **co-chair of several workshops in the field of Security, Mobility** and during the last years in IoT and Smart Cities. He is also associate editor of IEEE Trans SMC.Part B, **Security and Communication Networks Magazine** and has been special issue editor of IEE Proc. Communications, IJIPT journal and Computer Networks. He has also participated in **several standardization activities** being co-authors of some drafts about security and communications at the IETF, and participant of WG on ETSI (INS ING) and ISO WG. He has also been part of the initial team proposing to W3C the SIOC (Semantically-Interlinked Online Communities) submission.

Open Source Results:

Another indicator of his research contribution is the generation of technology knowledge transferred to Internet community, like **DYMOUM**(<http://masimum.dif.um.es/?Software:DYMOUM>), an implementation of the DYMO routing protocol proposed for MANETs; **OpenIKEv2** (Open source IKEv2 implementation, <http://openikev2.sourceforge.net/>) is an implementation under a free software license of the IKEv2 key management protocol; **UMU-PKiv6** (University of Murcia Public Key Infrastructure with IPv6 support, <http://pki.dif.um.es/>) is a public key infrastructure (PKI) acting as a test-bed to design and evaluate algorithm and protocols based on the concept of public key; **OpenXKMS** (<http://sourceforge.net/projects/xkms/>) is an open source implementation of the W3C Recommendation of the XML Key Management Specification (XKMS) 2.0.

Most Recent JCR Publications from 2019 to 2017

H2020 N°825618 – NGI_TRUST 3rd Open Call – 2019003

1. Architecture Of Security Association Establishment Based On Bootstrapping Technologies For Enabling Secure IoT Infrastructures. Authors: S Pérez, D Garcia-Carrillo, R Marín-López, JI Hernández-Ramos, R Marin-Perez, A Skarmeta. Future Generation Computer Systems 95, 570-585 (2019). **JCR Index: 4.639**
2. Toward a Cybersecurity Certification Framework for the Internet of Things. Authors: SN Matheu, JI Hernandez-Ramos, AF Skarmeta. IEEE Security & Privacy 17 (3), 66-76, 2019. **JCR Index: 1.596**
3. Security Management Architecture For NFV/SDN-Aware IoT Systems. Authors: Am Zarca, Jb Bernabe, R Trapero, A Skarmeta. IEEE Internet Of Things Journal 2019. **JCR Index: 5.863**
4. An Open IoT Platform For The Management And Analysis Of Energy Data. Authors: F Terroso-Saenz, A González-Vidal, Ap Ramallo-González, Af Skarmeta. Future Generation Computer Systems 1066-1079, 2019. **JCR Index: 4.639**
5. Surrogates: Virtual Obus To Foster 5g Vehicular Services Authors: J Santa, Pj Fernández, J Ortiz, R Sanchez-Iborra, Af Skarmeta. Electronics 8 (2), 117, 2019 **JCR Index: 2.110**
6. Risk-Based Automated Assessment And Testing For The Cybersecurity Certification And Labelling Of IoT Devices Authors: Sn Matheu-García, JI Hernández-Ramos, Af Skarmeta, G Baldini. Computer Standards & Interfaces 62, 64-83, 2019 **JCR Index: 1.465**
7. Plug-N-Harvest Architecture For Secure And Intelligent Management Of Near-Zero Energy Buildings. Authors: R Marin-Perez, It Michailidis, D Garcia-Carrillo, Cd Korkas, A Skarmeta. Sensors 19 (4), 843, 2019 **JCR Index:2.475**
8. Enabling Virtual AAA Management In SDN-Based IoT Networks. Authors: Am Zarca, D Garcia-Carrillo, Jb Bernabe, J Ortiz, R Marin-Perez, A Skarmeta. Sensors 19 (2), 295, 2019 **JCR Index: 2.475**
9. Lpwan-Based Vehicular Monitoring Platform With A Generic Ip Network Interface. Authors: J Santa, R Sanchez-Iborra, P Rodriguez-Rey, L Bernal-Escobedo, A Skarmeta. Sensors 19 (2), 264, 2019 **JCR Index: 2.475**
10. Tracking And Monitoring System Based On Lora Technology For Lightweight Boats. Authors: R Sanchez-Iborra, I G Liaño, C Simoes, E Couñago, A Skarmeta. Electronics 8 (1), 15, 2019 **JCR Index:2.110**
11. Smart Farming IoT Platform Based On Edge And Cloud Computing. Authors: Ma Zamora-Izquierdo, J Santa, Ja Martínez, V Martínez, Af Skarmeta. Biosystems Engineering 177, 4-17, 2019. **JCR Index: 2.325**
12. Overview Of Device Access Control In The IoT And Its Challenges. Authors: V Beltran, Af Skarmeta. IEEE Communications Magazine 57 (1), 154-160, 2019. **JCR Index: 9.27**
13. Evolving IoT Networks By The Confluence Of Mec And Lp-Wan Paradigms. Authors: R Sanchez-Iborra, J Sanchez-Gomez, A Skarmeta. Future Generation Computer Systems 88, 199-208, 2018. **JCR Index: 4.639**
14. Beats: Blocks Of Eigenvalues Algorithm For Time Series Segmentation. Authors: A Gonzalez-Vidal, P Barnaghi, Af Skarmeta. IEEE Transactions On Knowledge And Data Engineering 30 (11), 2051-2064, 2018. **JCR Index: 2.775**
15. Protecting Personal Data In IoT Platform Scenarios Through Encryption-Based Selective Disclosure. JI Hernández-Ramos, S Pérez, C Hennebert, Jb Bernabé, B Denis, A Skarmeta. Computer Communications 130, 20-37, 2018. **JCR Index: 2.613**
16. Enhancing IoT Security Through Network Softwarization And Virtual Security Appliances. Authors: A Molina Zarca, J Bernal Bernabe, I Farris, Y Khettab, T Taleb, A Skarmeta. International Journal Of Network Management 28 (5), E2038, 2018. **JCR Index: 1.34**
17. Special Issue On Management Of IoT. Authors: J Sá Silva, A Loureiro, A Skarmeta, F Boavida. International Journal Of Network Management 28 (5), E2032, 2018. **JCR Index: 1.34**
18. Enhancing Lorawan Security Through A Lightweight And Authenticated Key Management Approach. Authors: R Sanchez-Iborra, J Sánchez-Gómez, S Pérez, P Fernández, J Santa, A Skarmeta. Sensors 18 (6), 1833, 2018 **JCR Index: 2.110**
19. Performance Evaluation Of Lora Considering Scenario Conditions. Authors: R Sanchez-Iborra, J Sanchez-Gomez, J Ballesta-Viñas, Md Cano, A Skarmeta. Sensors 18 (3), 772, 2018 **JCR Index: 2.110**
20. Matching Federation Identities, The Edugain And Stork Approach. Authors: E Torroglosa, J Ortiz, A Skarmeta. Future Generation Computer Systems 80, 126-138, 2018. **JCR Index: 4.639**
21. Offloading Positioning Onto Network Edge. Authors: J Santa, Pj Fernández, R Sanchez-Iborra, J Ortiz, Af Skarmeta. Wireless Communications And Mobile Computing 2018. **JCR Index: 0.86**
22. A Lightweight And Flexible Encryption Scheme To Protect Sensitive Data In Smart Building Scenarios. Authors: S Pérez, JI Hernández-Ramos, Sn Matheu-García, D Rotondi, A Skarmeta. IEEE Access 11738-11750 2018. **JCR Index: 3.557**
23. Integration Of Anonymous Credential Systems In IoT Constrained Environments. Authors: Jlc Sanchez, Jb Bernabe, Af Skarmeta. IEEE Access 6, 4767-4778, 2018. **JCR Index: 3.557**

24. Secrbac: Secure Data In The Clouds. Authors: Jmm Pérez, Gm Pérez, Afs Gómez. IEEE Transactions On Services Computing 10 (5), 726-740, 2017. **JCR Index: 4.417**
25. A User-Centric Internet Of Things Platform To Empower Users For Managing Security And Privacy Concerns In The Internet Of Energy. Authors: Ja Martínez, JI Hernández-Ramos, V Beltrán, A Skarmeta, Pm Ruiz. International Journal Of Distributed Sensor Networks 13 (8), 2017 **JCR Index: 1.787**
26. Towards Seamless Inter-Technology Handovers In Vehicular Ipv6 Communications. Authors: Pj Fernández, J Santa, F Pereñíguez, Af Skarmeta. Computer Standards & Interfaces 52, 85-96, 2017 **JCR Index: 1.465**
27. Applicability Of Big Data Techniques To Smart Cities Deployments. Authors: Mv Moreno, F Terroso-Sáenz, A González-Vidal, M Valdés-Vela, A Skarmeta. IEEE Transactions On Industrial Informatics 13 (2), 800-809, 2017 **JCR Index: 5.43**
28. Army: Architecture For A Secure And Privacy-Aware Lifecycle Of Smart Objects In The Internet Of My Things. IEEE Communications Magazine, Vol. 54, Nº9, 28-35 (2017). Autores: Hernández Ramos, J. L.; Bernal Bernabe, J.; Antonio F. Gómez Skarmeta. **JCR Index: 5.125**

Recent International Projects (FP7, H2020) Funded By European Commission

1. H2020-EE-2014-2-Ria Design Of An Innovative Energy-Aware It Ecosystem For Motivating Behavioural Changes Towards The Ado.
2. H2020-FCT-2015 Reliable European Identity Ecosystem.
3. H2020-IoT-2016-2017 IoTcrawler.
4. H2020-ICT-2018-2 Cyber Security Network Of Competence Centres For Europe
5. H2020-DS-SC7-2017 Oblivious Identity Management For Private And User-Friendly Services.
6. ICT-2016-1 5gfire1-Exp-1 Virtual Obus And Hybrid Communications To Foster 5g Vehicular Services.
7. H2020-ICT-2018-2 5g For Cooperative & Connected Automated Mobility On X-Border Corridors.
8. H2020-DS-LEIT-2016 Advanced Networked Agents For Security And Trust Assessment in CPS/IoT Architectures
9. H2020-Aries Reliable European Identity Ecosystem.
10. Enabling Sdn Experimentation in Wireless Testbeds Exploiting future Internet Infrastructure In South Korea.
11. Design Of An Innovative Energy-Aware It Ecosystem For Motivating Behavioural Changes.
12. FP7-Smartcities-2013-10-609112 SocioTal.
13. FP7-Smartcities-2013-10-609062. Secure And Smarter Cities Data Management Smartie.
14. FP7-ICT-2011-7-288445 Universal Integration Of The Internet Of Things Through An Ipv6-Based Service Oriented Architecture.
15. FP7-IST 027002 Enabling Efficient And Operational Mobility In Large Heterogeneous Ip Networks.
16. 7PM-ICT-2009-6-270447 European Field Operational Test On Safe, Intelligent And Sustainable Road Operation
17. FP7-ICT-2011-8-317731. Interoperable Trust Assurance Infrastructure. Start: 01/11/2012, End: 30/04/2015
18. FP7-Infrastructure-2009 Multigigabit European Academic Network. Start: 01/04/2009, End: 31/03/2015
19. FP7-People-2010-Cofund Incoming Mobility Programme Action. Start: 01/11/2011, End: 31/10/2015
20. CIP-ICT-PSP-5 Secure Identity Across Borders Linked 2.0. Start: 01/04/2012, End: 30/09/2015
21. FP7-ICT-2011-7 Openlab: Extending Fire Testbeds And Tools. Start: 01/09/2011, End: 30/06/2014

Relevant Patents

1. System And Telematic Method For Security In The Circulation Of Vehicles. P201631588. Agente: Herrero Y Asociados. Register Date: 14/12/2016.
2. Method And System For The Efficient Use Of Resources And Presence Control In Classrooms. P201500548. Agente: Herrero & Asociados. Register Date: 15/07/2015.
3. Method And System For The Flexible Configuration Of Remote Control And Monitoring Devices. P201700049. Agente: Herrero & Asociados. Register Date: 13/01/2017.
4. Procedure To Predict The Energy Consumption Of Environmental Climate Control In Buildings. Agente: Herrero & Asociados. Register Date: 07/03/2017.
5. System, Device And Method For The Obtaining Of Encapsulated Objects. P201230267. Agente: Abril Abogados. Register Date: 22/02/2012.
6. Mobility-Aware Mesh Construction Algorithm For Low Data-Overhead Multicast Ad Hoc Routing. Agente: Steven M. Hoffberg. Register Date: 29/11/2006.
7. Integral System Of Control, Security And Home Automation In Intelligent Buildings. P200802506. Agente: Elzaburu. Register Date: 28/08/2008.
8. Re-Authentication Procedure. P200930015. Agente: Elzaburu. Register Date: 27/03/2009.
9. Electronic Device For Remote Stations For Remote Control. Register Date: 21/12/2006. P200603241

Part A. Personal Data

Name	Rafael Marin Perez		
DNI/NIE/Passport	77707950N	Years	39
Id of researcher	ResearcherGate	https://www.researchgate.net/profile/Rafael_Marin-Perez	
	Orcid Code	https://orcid.org/0000-0002-8521-1864	

A.1. Current Professional Situation

Entity	Odin Solutions SL		
Department	Research and Innovation		
Address	Calle Peru 5, Piso 3, Ofician 5, 30850, Alcantarilla, Pol. Oeste, Murcia		
Phone	+34 868123395	Email	rmarin@um.es
Position	Senior Researcher	Start Date	1/2/2015

A.2. Academic Education

Degree in computer science	University of Murcia, Spain	2006
PhD in computer science	University of Murcia, Spain	2012

A.3. General KPI of the quality of scientific production

Total cites: 525 (according to Google Scholar)	Number of JCR publications: 8
Total JCR publications in first quartile (Q1): 6	Number of int. congress: 7
Index h: 11 (according to Google Scholar).	Member of Technical Program Committee: 7
Number of international R&D projects: 10	Number of national R&D projects: 8

CV Summary:

He received the M.S. degree in Computer Science from the University of Murcia in 2006 and his Ph.D. (Hons.) in Computer Science at University of Murcia in 2012. Since 2006, he has worked as full-time researcher on more 10 international projects in the field of **Wireless Sensor Networks, Internet of Things, Security/Privacy** such as Fed4IoT, Plug-n-Harvest, ANASTACIA, IoTcrawler, Cpaas, ARMOUR, SMARTIE, SOCIOTAL, IoT6 as well as more 8 national R&D projects such as IoT@AS, SIROCO, SAVIA, HospiSegur, MCiudad, Platon, and MARTA. He gained his expertise on the innovation areas of low-power wireless technologies (Zigbee, Sigfox, LORA and 5G), IoT communication protocols (6lowpan, MQTT, COAP, etc) and security/privacy mechanisms (i.e. Bootstrapping) for constrained devices. The main quality indicators are the **relevance of congresses and journals** where their scientific-technological research has been published in the area of telecommunications and security. We highlight congresses such as IEEE Mobile Ad-hoc Sensor Systems or IEEE Local Computer Networks, as well as **high impact journals** such as MDPI Sensors (JCR 2,475), Pervasive and Mobile Computing (JCR 3,009), IEEE Communications Magazine (JCR 4,007) and Future Generation Computer Systems (JCR 4.968). In addition, Rafael participates in the **technical program committees of international journals/congresses** such as IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE World Forum on Internet of Things (WF-IoT), Global Internet of Things (GloT) or European Conference on Networks and Communications (EuCNC) co-organized by IEEE Communications Society and European Association for Signal Processing and European Commission. In addition, he collaborates in **standardization activities** of new IoT technologies in international entities where OdinS is a member such as International IoT Forum and AIOTI (Alliance for internet of things innovation). Moreover, he participates in standardization committees such as Technical Committee 318 (Irrigation telecontrol systems) within ISO (International Organization for Standardization) and ISG CIM (cross-sector Context Information Management) within ETSI (European Telecommunications Standards Institute). In OdinS he received relevant international/national awards such as National SocInfo 2014 for SmartCities Solutions, National Startup4Cities 2014, National EnerTIC 2014 and International IoT360 2014 (IoT Summit).

Recent JCR Publications

1. Architecture Of Security Association Establishment Based On Bootstrapping Technologies For Enabling Secure IoT Infrastructures. Authors: S Pérez, D Garcia-Carrillo, R Marín-López, JI Hernández-Ramos, R Marin-Perez, A Skarmeta. Future Generation Computer Systems 95, 570-585 (2019). **JCR Index: 4.693**
2. Plug-N-Harvest Architecture For Secure And Intelligent Management Of Near-Zero Energy Buildings. Authors: R Marin-Perez, It Michailidis, D Garcia-Carrillo, Cd Korkas, A Skarmeta. Sensors 19 (4), 843, 2019. **JCR Index: 2.475**
3. Enabling Virtual AAA Management In SDN-Based IoT Networks. Authors: A Zarca, D. Garcia-Carrillo, J. Bernabe, J Ortiz, R Marin-Perez, A Skarmeta. Sensors, 295, 2019. **JCR Index: 2.475**

4. Pablo Lopez; David Fernandez; Rafael Marin Perez; Antonio Jara; Antonio Skarmeta. Scalable Oriented-Service Architecture For Heterogeneous And Ubiquitous IoT Domains. Pervasive And Mobile Computing. Elsevier, 2015. **JCR Index: 2.693**
5. A Real-Time Measurement System For Long-Life Flood Monitoring And Warning Applications. Authors: Rafael Marin-Perez; Javier Garcia-Pintado; Antonio F. Gomez-Skarmeta. Mdpi Sensors. 12 No.4, Pp. 4213-4236. 2013. **JCR Index: 2.475**
6. Beacon-Less Geographic Multicast Routing In A Real-World Wireless Sensor Network Testbed. Authors: Juan A. Sanchez; Rafael Marin-Perez; Pedro M. Ruiz. Wireless Networks. 2012. **JCR Index: 1.055**
7. Beacon-Less Geographic Routing Made Practical: Challenges, Design Guidelines, And Protocols. Authors: Juan A. Sanchez; Pedro M. Ruiz; Rafael Marin-Perez. IEEE Communications Magazine. 47, No. 8, Pp. 85-91, 2011 **JCR Index: 4.007**
8. Beacon-Less Geographic Routing In Real Wireless Sensor Networks. Authors: Juan A. Sanchez; Rafael Marin-Perez; Pedro M. Ruiz. Journal On Computer Science And Tehcnology (Jcst). 23, No.3 Pp. 438-450, 2011 **JCR Index: 0.672**

Recent International Projects (FP7, H2020) Funded By European Commision

1. H2020 Demeter: Building An Interoperable, Data-Driven, Innovative & Sustainable European Agri-Food Sector. Total: 9.576.213 €
2. H2020 Fed4IoT: Federating IoT And Cloud Infrastructures To Provide Scalable And Interoperable Smart Cities Applications. Total: 1.499.378 €
3. H2020 IoTcrawler: A Search Engine For The Internet Of Things. Total: 4.997.137 €
4. H2020 Anastacia: Advanced Networked Agents For Security And Trust Assessment In Cps-IoT Architectures. Total: 5.420.208 €
5. H2020 Plug-N-Play Passive And Active Multi-Modal Energy Harvesting Systems, Circular Economy By Design, With High Replicability For Self-Sufficient DistrICTs Near-Zero Buildings. Total: 6.896.147 €
6. H2020 City Platform As A Service (Cpaas). Total: 1.786.407 €
7. H2020 Armour: Large-Scale Experiments Of IoT Security & Trust. Total: 1.999.558 €
8. FP7 Smartie: Secure And Smarter Cities Data Management. Total: 3.286.144 €
9. FP7 SocioTal: Reliable, Smart And Secure Internet Of Things For Smart Cities. Total: 3.687.350 €
10. FP7 IoT6: Universal Integration Of The Internet Of Things Through An Ipv6-Based Service Oriented Architecture Enabling Heterogeneous Components Interoperability. Total: 4.140.000 €

Recent National R&D Projects

1. IoT@AS: Internet Of Things & Agrospace. Financial Entity: Cdti Interconnecta 2016. Start: 01/10/2016-31/03/2019 Total: 1.489.479 €
2. Siroco: Sistema De Información Industrial Formado Por Componentes Activos Usando Internet De Las Cosas E Internet De Los Servicios. Financial Entity: Cdti Interconnecta 2016. Start: 01/10/2016-31/03/2019 Total: 1.397.563 €
3. Marta: Movilidad Y Automoción Con Redes De Transporte Avanzadas. Main Researchers: Pedro Miguel Ruiz And Rafael Marin Perez. Financial Entity: Ministerio De Ciencia E Innovación. Start: 01/10/2011-31/12/2014 Total: 35.000.000 €
4. Hospisegur: Sistema De Seguridad Para Pacientes Hospitalizados. Main Researchers: Pedro Miguel Ruiz And Rafael Marin Perez. Financial Entity: Ministerio De Industria, Comercio Y Turismo (Fit-350301-2007-15). Start: 01/01/2007 - 31/12/2008 Total: 98.218 €
5. M-Ciudad: Investigación Tecnológica En Comunicaciones Móviles Para Posibilitar La Movilidad Y Ubicuidad En Los Servicios Urbanos Mediante Redes De Sensores Inalambricas. Main Researchers: Antonio Skarmeta And Rafael Marin Perez. Financial Entity: Ministerio De Industria, Comercio Y Turismo (Profit-Fit-330503-2006-2) Start: 01/01/2006 - 28/02/2008
6. Savia: Sistema Avanzado De Visitas Interactivas Asistidas. Main Researchers: Pedro Miguel Ruiz And Rafael Marin Perez. Financial Entity: Ministerio De Industria Y Turismo (Cit-410000-2005-1). Start: 01/01/2005 - 31/12/2005
7. Sistema De Riego Avanzado Basado En Industria 4.0. Main Researchers: Rafael Marin Perez. Company: Riegos Y Tecnología SI (Ritec). Financial Entity: Instituto De Fomento De La Region De Murcia. Start: 01/02/2017 Duration 1 Year.

8. Platon IoT Platform. Main Researcher: Antonio Skarmeta Gomez; Rafael Marin Perez; Juan Antonio Martinez Navarro. Financial Entity: Instituto De Fomento De La Region De Murcia. Start: 01/09/2016 Duration: 1 Year. Total: 149.765 €

Recent International Conferences

1. EAP-based bootstrapping for secondary service authentication to integrate IoT into 5G networks. Authors: Dan Garcia-Carrillo, Jesus Sanchez-Gomez, Rafael Marin-Perez and Antonio Skarmeta. The 4th International Symposium on Mobile Internet Security (MobiSec 2019). Core Index: B
2. Virtual AAA Security Function In Nfv/Sdn-Enabled IoT Scenarios. Authors: Alejandro Molina Zarca; Dan Garcia Carrillo; Jorge Bernal Bernabe; Jordi Ortiz; Rafael Marin Perez; Antonio Skarmeta Gómez. Global IoT Summit 2018. Bilbao, Spain, 06/06/2018. IEEE Communication Society. Core Index: A
3. A Simple Self-Protected Beaconless Geographic Routing For Wireless Sensor Networks. Authors: Rafael Marin-Perez; Pedro M. Ruiz. Juan A. Sanchez; 8th IEEE International Conference On Mobile Ad-Hoc And Sensor Systems (IEEE Mass 2011) 7/10/2011. Institute Of Electrical And Electronics Engineers. Core Index: A
4. Effective Geographic Routing In Wireless Sensor Networks With Inaccurate Location Information. 10th International Conference On Ad Hoc Networks And Wireless (Adhoc-Now). 18/07/2011. Institute Of Electrical And Electronics Engineers. Core Index: B
5. Bruma: Beacon-Less Geographic Routing For Multicast Applications. Authors: Rafael Marin-Perez; Pedro M. Ruiz. Juan A. Sanchez; 34th IEEE International Conference On Local Computer Networks (LCN) 2009. Institute Of Electrical And Electronics Engineers. Core Index: A
6. Beacon-Less On Demand Strategy For Geographic Routing In Wireless Sensor Networks. Authors: Rafael Marin-Perez; Pedro M. Ruiz. Juan A. Sanchez; 4th IEEE Conference On Mobile Ad-Doc And Sensor Systems (Mass 2007). Core Index: A.
7. A Remote Measurement System For Hydrological Monitoring Network. Authors: Rafael Marin Perez; Antonio Skarmeta Gómez. The Second International Workshop On Sensing Technologies In Agriculture, Forestry And Environment. 04/2011 University Of Novi Sad.
8. Flood Protection System For Mediterranean Environment. Authors: Rafael Marin Perez; Antonio Skarmeta Gómez. Multi-Conference Resouk Emuni 10/03/2011.

Member Of Technical Program Committees

1. European Conference On Networks And Communications (Eucnc). Organizer: IEEE Communications Society. 13/11/2018
2. Global Internet of Things Summit (GloTs). Organizer: IEEE IoT Communications Society. 09/04/2018
3. Journal Of Wireless Networks. Organizer: Institute Of Electrical And Electronics Engineers. 01/03/2018
4. International Journal Of Distributed Sensor Networks. Organizer: Hindawi Publishing Corporation 28/02/2018
5. IEEE World Forum On Internet Of Things (Wf-IoT). Organizer: Institute Of Electrical And Electronics Engineers. 16/03/2015
6. IEEE Transactions On Wireless Communications. Organizer: Institute Of Electrical And Electronics Engineers (IEEE). 07/11/2014
7. IEEE Transactions On Wireless Communications. Organizer: Institute Of Electrical And Electronics Engineers 05/06/2014

Personal Research Grants

- Postdoctoral Grant Ptq-15-08003 – Torres Quevedo By The Ministry Of Economy And Competitiveness Of Spain.

Part A. Personal Data

Name	Dan Garcia Carrillo		
DNI/NIE/Passport	48633263Q	Years	31
Id of researcher	ResearcherGate	https://www.researchgate.net/profile/Dan_Garcia_Carrillo	
	Orcid Code	https://orcid.org/0000-0003-0803-1672	

A.1. Current Professional Situation

Entity	Odin Solutions SL		
Department	Research and Innovation		
Address	Calle Peru 5, Piso 3, Ofician 5, 30850, Alcantarilla, Pol. Oeste, Murcia		
Phone	+34 868123395	Email	dgarcia@odins.es
Position	Postdoctoral Researcher	Start Date	11/10/2018

A.2. Academic Education

BSc in computer science	University of Murcia, Spain	2012
Master's in computer science	University of Murcia, Spain	2014
PhD in computer science	University of Murcia, Spain	2018

A.3. General KPI of the quality of scientific production

Total cites: 118 (according to Google Scholar)	Number of property registers: 1
Total JCR publications in first quartile (Q1): 4	Number of JCR publications: 7
Index h: 6 (according to Google Scholar).	Number of int. congress: 5
Number of projects: 4	Member of Technical Program Committee: 1

CV Summary: Dan Garcia Carrillo was born in Murcia in 1988. He obtained the degree in computer science in University of Murcia in 2012 and a master's in information and communication technologies in 2014 and the doctorate in computer science in 2018. He obtained his Ph.D. with the international as well as the industrial honors and finished the doctorate in Odin Solutions S.L. His industrial doctorate is being carried out under the Spanish Industrial Doctorate grant which is a relevant national grant. He is currently a post doctorate researcher in OdinS. His research is focused on internet technologies for security, privacy and trust as showed the most of the publications and also the title of his thesis, "**A COAP-BASED BOOTSTRAPPING SERVICE FOR LARGE-SCALE INTERNET-OF-THINGS NETWORKS**".

Since he started his research career, he has participated in international R&D projects funded by European Commission in the program FP7 and H2020. In particular, Dan has participated in **4 European projects** (i.e. SMARTIE, SocloTal, ANASTACIA and Plug-N-Harvest) related to security, privacy and trust technologies for cross-domain sectors such as Smart Cities, Industry 4.0, Smart Agriculture, etc.

Since 2014, he have contributed and contributes to **several standardization activities** at the Internet Engineering Task Force (IETF) being co-authors of 6 drafts in innovative areas related to **security and bootstrapping for decentralized Internet infrastructures**. He holds one property registry. He is the author of **7 JCR publications, 4 International Congresses, 2 book chapters and 5 Internet Drafts**. He was member of technical program committee of SPIoT International Congress and has performed a review for a book proposal. Moreover, Dan has assisted 4 years in the Faculty of Computer Science of the University of Murcia under "Venia Docendi" in subjects such as *Advanced Networks* and *Telematic Services*.

Recent JCR Publications

1. Salvador Perez, Dan Garcia-Carrillo, Rafael Marn-Lopez, Jos L. Hernandez-Ramos, Rafael Marin-Prez, And Antonio F. Skarmeta. Architecture Of Security Association Establishment Based On Bootstrapping Technologies For Enabling Secure IoT Infrastructures. Future Generation Computer Systems, 95:570 – 585, 2019. **Jcr Index: 4.639**

2. Rafael Marin-Perez, Iakovos T Michailidis, Dan Garcia-Carrillo, Christos D Korkas, Elias B Kosmatopoulos, And Antonio Skarmeta. Plug-N-Harvest Architecture For Secure And Intelligent Management Of Near-Zero Energy Buildings. *Sensors*, 19(4):843, 2019 **Jcr Index:2.475**
3. Alejandro Molina Zarca, Dan Garcia-Carrillo, Jorge Bernal Bernabe, Jordi Ortiz, Rafael Marin-Perez, And Antonio Skarmeta. Enabling Virtual Aaa Management In Sdn-Based IoT Networks. *Sensors*, 19(2):295, 2019. **Jcr Index: 2.475**
4. Dan Garcia-Carrillo And Rafael Marin-Lopez. Multihop Bootstrapping With Eap Through Coap Intermediaries For IoT. *IEEE Internet Of Things Journal*, 5(5):4003–4017, 2018 . **Jcr Index: 2.475**
5. Dan Garcia-Carrillo, Rafael Marin-Lopez, Arunprabhu Kandasamy, And Alexander Pelov. A Coap-Based Network Access Authentication Service For Low-Power Wide Area Networks: Lo-Coap-Eap. *Sensors*, 17(11):2646, 2017. **Jcr Index: 2.475**
6. Dan Garcia-Carrillo And Rafael Marin-Lopez. Lightweight Coap-Based Bootstrapping Service For The Internet Of Things. *Sensors*, 16(3):358, 2016. . **Jcr Index: 2.475**
7. Jose L. Hernandez-Ramos, M VICTORIA Moreno, Jorge Bernal Bernabe, Dan Garcia Carrillo, And Antonio F Skarmeta. Safir: Secure Access Framework For IoT-Enabled Services On Smart Buildings. *Journal Of Computer And System Sciences*, 81(8):1452–1463, 2015 . **Jcr Index: 1.497**

Recent International Projects (FP7, H2020) funded by European Commision

1. FP7-Smartcities-2013-10-609062. Secure And Smarter Cities Data Management Smartie. Entity: European Commision.
2. FP7-Smartcities-2013-10-609112 SocloTal. Entity: European Commission.
3. H2020-EEB-2017. Plug-N-Play Passive And Active Multi-Modal Energy Harvesting Systems, Circular Economy By Design, With High Replicability For Self-Sufficient Districts Near-Zero Buildings
4. H2020-DS-LEIT-2016 ANASTACIA: Advanced Networked Agents For Security And Trust Assessment In CPS-IoT Architectures.

Recent International Conferences

1. EAP-based bootstrapping for secondary service authentication to integrate IoT into 5G networks. Authors: Dan Garcia-Carrillo, Jesus Sanchez-Gomez, Rafael Marin-Perez and Antonio Skarmeta. The 4th International Symposium on Mobile Internet Security (MobiSec 2019). Core Index: B
2. Jose L Hernandez-Ramos, Dan Garcia Carrillo, Rafael Marin-Lopez, And Antonio F Skarmeta. Dynamic Security Credentials Pana-Based Provisioning For IoT Smart Objects. In 2015 IEEE 2nd World Forum On Internet Of Things (Wf-IoT), Pages 783–788. IEEE, 2015
3. Jens-Matthias Bohli, Antonio Skarmeta, M Victoria Moreno, Dan Garcia, And Peter Langendorfer. Smartie Project: Secure IoT Data Management For Smart Cities. In 2015 International Conference On Recent Advances In Internet Of Things (RIoT), Pages 1–6. IEEE, 2015.
4. Ivan Farris, Jorge Bernal Bernabe, Nassima Toumi, D Garcia-Carrillo, Tarik Taleb, A Skarmeta, And B Sahlin. Towards Provisioning Of Sdn/Nfv-Based Security Enablers For Integrated Protection Of IoT Systems. In 2017 IEEE Conference On Standards For Communications And Networking (Cscn), Pages 169–174. IEEE, 2017
5. Alejandro Molina Zarca, Dan Garcia-Carrillo, Jorge Bernal Bernabe, Jordi Ortiz, Rafael Marin-Perez, And Antonio Skarmeta. Managing Aaa In Nfv/Sdn-Enabled IoT Scenarios. In 2018 Global Internet Of Things Summit (GloTs), Pages 1–7. IEEE, 2018

Book Chapters

1. Antonio Skarmeta, Dan Garcia Carrillo, And Alexis Olivereau. End-Node Security. In *Internet Of Things Security And Data Protection*, Pages 45–69. Springer, 2019.
2. Jose L Hernandez-Ramos, Dan Garcia Carrillo, Antonio Skarmeta, Fabio Gonçalves, Luis Cortesão, Jens-Matthias Bohli, And Martin Bauer. Smartie: A Secure Platform For Smart Cities And IoT. *Eng. Secure Intern. Things Syst*, 2:75, 2016

Internet Drafts of IETF

1. Behcet Sarikaya, Mohit Sethi, And Dan Garcia-Carrillo. **Secure IoT Bootstrapping**. Internet-Draft Draft-Sarikaya-T2trg-Sbootstrapping-06, Internet Engineering Task Force, January 2019. **Work In Progress**.
2. Rafael Lopez And Dan Garcia-Carrillo. **EAP-Based Authentication Service For COAP**. Internet-Draft Draft-Marin-Ace-Wg-Coap-Eap-06, Internet Engineering Task Force, October 2017. **Work In Progress**.
3. Dan Garcia-Carrillo, Rafael Lopez, Arunprabhu Kandasamy, And Alexander Pelov. **Lorawan Authentication In Radius**. Internet-Draft Draft-Garcia-Radext-Radius-Lorawan-03, Internet Engineering Task Force, May 2017. **Work In Progress**.
4. Dan Garcia-Carrillo, Sara Nieves Matheu Garcia, And Rafael Lopez. **Application Layer Security For COAP Using The (D)TLS Record Layer**. Internet-Draft Draft-Garcia-Core-App-Layer-Sec-With-Dtls-Record-00, Internet Engineering Task Force, December 2016.
5. Dan Garcia-Carrillo, Rafael Lopez, Arunprabhu Kandasamy, And Alexander Pelov. **Lorawan Authentication In Diameter**. Internet-Draft Draft-Garcia-Dime-Diameter-Lorawan-00, Internet Engineering Task Force, May 2016.

Personal Research Grants

- Industrial Doctorate By The Ministry Of Economy And Competitiveness Of Spain - Di-16-08432

Member of Technical Program Committees

- International Symposium On Security & Privacy On Internet Of Things - SpIoT 2018

Part A. Personal Data

Name	Mirko Ross	
Professional Profile	LinkedIn	https://www.linkedin.com/in/mirko-ross-4241125/

A.1. Current Professional Situation

Entity	Digital Worx GmbH		
Department	Research and Innovation		
Address	Schulze-Delitzsch-Str. 16 70565 Stuttgart Germany		
Phone	+49 711 2204093 0	Email	m.ross@digital-worx.de
Position	Chief Executive Officer (CEO)	Start Date	1/10/2010

A.2. Academic Education

Dipl.-Ing. (FH)	University of Applied Science Nürtingen	1998
Assistant Professor	University of Applied Science, Heilbronn	2012

A.3. General KPI of the quality of professional career

Number of R&D projects: 10	Number of magazine publications: > 5
Number of Private contracts: > 30	Founded Companies: 3
Number of Awards: 8	

CV Summary:

Mirko was born 1972 in Göppingen, Germany. 1998 he graduated at University of Applied Science Nürtingen with excellence and is holding a degree Dipl.-Ing. (FH). Since 1998 he has founded 3 companies in the ICT sector. Since 2017 he is technical lead Advisor at Blackpin Secure Communication and Member of the advisory board of DigitCode a company focusing the improvement of reliable communication in the Internet of Things. From 2012 to 2019, he taught Web Engineering and mobile Software Development at Heilbronn University. Mirko is involved in public and private research activities for open standards and disruptive business models in IoT sector. He is member of the Internet Of Things Council, a worldwide IoT think tank. Also he contributed to AIOTI – Alliance for Internet of Things Innovation. Since 2018 he is Co-Chair of the AIOTI Working Group Distributed Ledger. In the European Commission's Future Internet program he supported as a business coach startups in the fields of eHealth and industrial IoT. Since 2016 until now he is coaching SME and Startups in the European SME Instrument. Since 2017 Mirko is a member of the IoT Security Expert Group of the European Agency of Network and Information Security [ENISA](#). And Mirko is project coordinator of the digital health research project [MITASSIST](#). He is a member of the [IOTA](#) Evangelist Network (IEN) to support Blockchain and Distributed Ledger technologies. Together with international Partners he is working on secure search engine for IoT networks at the HORIZON2020 project [IoTcrawler](#). Also since 2018 Mirko is a reviewer for R&D projects under HORIZON2020. Mirko is a well-practiced international speaker and coach on the field of Open Innovation, Internet of Things, Security and disruptive business modeling. With [asvin.io](#) he cofounded a new venture to provide secure open source based update and patch delivery for IoT networks.

Most Recent Publications

1. Ross, Walbert (2009) «Castogo, der ortsunabhängige Reiseführer», A digital Lifestyle
2. Ross (2015) «Das Content Management-System als Backend-Lösung: iBeacons mit TYPO3 verwalten und steuern», T3N Magazine
3. Ross (2014) «Bluetooth stärkt das Serviceteam», VDI Nachrichten

4. Ross (2018) «Why Blockchain is a high potential gamechanger in utility industries», European Energy Innovation Magazine
5. Ross (2018) «Europas Verordnung zur IoT Sicherheit ist Zahnlos», Heise Verlag

Recent International/National R&D Projects

1. 2006 Colamo.org Building the Next Generation Collaborative Mobile Groupware. Funded by Bmbf ProINNO I
2. 2009 OSS Maschinenbau Netzwerk Open Source im Maschinenbau. Funded by Bmbf ZIM
3. 2007 Moderator at TASK - Software-Lieferketten (Funded by MWF BW)
4. 2014 Coordinator at iBeacon on industrial Production at Fraunhofer test plant
5. 2014 Coordinator for Dimago mhealth Solution in FICHE Fiware Accelerator
6. 2014 Coordinator for CoJob3D Solution in FABulous Fiware Accelerator
7. 2017 Consortium Coordinator at MITASSIST Project, funded by Bmbf Germany
8. 2017 Coordination for Industry 4.0 best practice applications for Industry 4.0 Lighthouse project Arena2036
9. H2020-INNOSUP-2014 KATANA
10. H2020-IOT-2016-2017 IOTCRAWLER

Most Recent Private Contracts for R&D Projects (selected examples of +30)

1. 2011 Project lead HELLER Services Knowledge Management System for machinery
2. 2012 Project lead B/S/H Augmented Reality Prototyping for mobile services at BOSCH - B/S/H
3. 2014 Project Lead WAFIOS AG Location awareness system for mobile services on smart manufacturing
4. 2016-2019 Initiator of The Things Network Stuttgart, operating an open Network with rnd 50 LoRa Gateways
5. 2016-2019 preferred supplier by BASF AG to increase global productivity of mobile real estate assesment
6. 2017 Supplier of 3 Industry 4.0 best practice applications for Industry 4.0 Lighthouse project Arena2036
7. 2018-2019 preferred supplier for mobile industrial productivity solutions at PORSCHE AG production line ptz.
8. 2018-2019 Co-Creation partner for blockchain based peer-to-peer energy applicatons at EVM AG
9. 2018-2019 Partnership with SIEMENS AG to increase Cybersecurity in Industry 4.0

International Awards

1. 2014 industry 4.0 solutions rated to the top 30 in Europe by 3D accelerator FABulous
2. 2014 selected as top 30 European Startup Company by European Investors Gate (EIG)
3. 2014 wearable solution selected as top 40 ehealth solution in Europe by FICHE Accelerator
4. 2016 Excellence Industrie 4.0 Award by Alliance 4.0 for mobile industrial content awareness applications
5. 2018 Selected Blockchain IoT Solution Provider by Dubai Future Accelerator Cohort 5
6. 2018 Top 10 German tech influencer rated by Right Relevance
7. 2019 2nd. Prize Award b2b Accelerator for Blockchain based IoT Security with asvin.io
8. 2019 Special Jury Award with asvin.io at Tokio FIBC (Financial Innovation Business Conference)

Part A. Personal Data

Name	Silke Capo	
Professional Profile	LinkedIn	https://www.linkedin.com/in/silke-capo-3452a7b4/

A.1. Current Professional Situation

Entity	Digital Worx GmbH		
Department	Research and Innovation		
Address	Schulze-Delitzsch-Str. 16 70565 Stuttgart Germany		
Phone	+49 711 2204093 0	Email	s.capo@digital-worx.de
Position	Senior Software Developer	Start Date	1/10/2011

A.2. Academic Education

Master Degree	University Ludwigsburg	1999
---------------	------------------------	------

A.3. General KPI of the quality of scientific and professional work

Number of R&D public projects: 7	Number of Awards: 7
Number of R&D private contracts: > 20	

CV Summary:

In 1998 Silke graduated at University of Applied Science Ludwigsburg. In 1999 she started working as software developer with focus on web-application and e-business. Since 2011 Silke is working as senior software developer and project consultant at digital worx, with a strong focus on the areas of innovations platforms, blockchain, distributed ledgers, etc. She is trained developer for agile Software-Development with SCRUM Methodology and technical supervisor for software development at digital worx's innovation projects under HORIZON2020 and national research projects. During her professional career, she has participated on the implementation and validation of more 20 R&D private contracts and 7 international/national R&D projects achieving 7 international awards in the area of blockchain and IoT solutions. Moreover, Silke has high experience in Distributed Ledger and Blockchain-based developments so as InterPlanetary File System (IPFS) for software patching distribution and vulnerabilities management.

Recent International/National R&D Projects

1. 2014 Senior Developer iBeacon on industrial Production at Fraunhofer test plant
2. 2014 Senior Developer for Dimago mhealth Solution in FICHE Fiware Accelerator
3. 2014 Senior Developer for CoJob3D Solution in FABolous Fiware Accelerator
4. 2017 Senior Developer at MITASSIST Project, funded by Bmbf Germany
5. 2017 Senior Developer for Industry 4.0 best practice applications for Industry 4.0 Lighthouse project Arena2036
6. H2020-INNOSUP-2014 KATANA
7. H2020-IOT-2016-2017 IOTCRAWLER.

Most Recent Private Contracts for R&D Projects (selected examples of +20)

1. 2011 Developer HELLER Services Knowledge Management System for machinery
2. 2012 Developer B/S/H Augmented Reality Prototyping for mobile services at BOSCH - B/S/H

3. 2014 Senior Developer WAFIOS AG Location awareness system for mobile services on smart manufacturing
4. 2014 Senior Developer for KALLFASS Machining video data repository
5. 2014 Senior Developer for HELLER Machining product configuration
6. 2014 Senior Developer for Bauknecht / Whirlpool world online service portal
7. 2014-2019 Senior Software Developer for online product configuration precitec GmbH
8. 2018-2019 Senior Developer for mobile industrial productivity solutions at PORSCHE AG production line ptz.
9. 2018-2019 Senior Developer for blockchain based peer-to-peer energy applications at EVM AG
10. 2018-2019 Senior Developer for asvin.io GUI / UX

International Awards

1. 2014 industry 4.0 solutions rated to the top 30 in Europe by 3D accelerator FABulous
2. 2014 selected as top 30 European Startup Company by European Investors Gate (EIG)
3. 2014 wearable solution selected as top 40 ehealth solution in Europe by fiche Accelerator
4. 2016 Excellence Industrie 4.0 Award by Alliance 4.0 for mobile industrial content awareness applications
5. 2018 Selected Blockchain IoT Solution Provider by Dubai Future Accelerator Cohort 5
6. 2019 2nd. Prize Award b2b Accelerator for Blockchain based IoT Security with asvin.io
7. 2019 Special Jury Award with asvin.io at Tokio FIBC (Financial Innovation Business Conference)

Part A. Personal Data

Name	Mihaly Virag	
Professional Profile	LinkedIn	https://www.linkedin.com/in/mihaly-virag-8b6b9933/

A.1. Current Professional Situation

Entity	Digital Worx GmbH		
Department	Research and Innovation		
Address	Schulze-Delitzsch-Str. 16 70565 Stuttgart Germany		
Phone	+49 711 2204093 0	Email	m.virag@digital-worx.de
Position	Senior Software Developer		Start Date 1/10/2011

A.2. Academic Education

Degree in Computer Science	University Gabor Denes	2001
----------------------------	------------------------	------

A.3. General KPI of the quality of scientific and professional work

Number of R&D public projects: 7	Number of Awards: 7
Number of R&D private contracts: > 15	

CV Summary:

In 2001 he obtained the degree in Computer Science in University Gabor Denes, Budapest. From 2001 to 2010, he worked as Web Developer and Freelance System Administrator (Novell Netware, Windows 2000), Project Management, Lecture, Project virtual Market of the Hungarian National Institute of Vocational Education (NIVE) supported by the European Committee in the framework of Leonardo da Vinci cooperation programme), Lecturer Computer Science at University krudy Gyula, Hungary and Supervisor at ECDL Commision. Since 2011, he is senior Software-Architect and Consultant in Digital Worx. Mihaly is a trained developer for agile Software-Development with SCRUM Methodology and technical supervisor for software development at innovation projects under HORIZON2020 and national research programs. During his career, he has participated on the development and deployment of software solutions in more 15 R&D private contracts and 7 international/national R&D projects achieving 7 international awards in the area of blockchain and IoT. Furthermore Mihaly is a skilled architect for Distributed Ledger and Blockchain-based developments so as InterPlanetary File System (IPFS) for software patching distribution.

Recent International/National R&D Projects

1. 2014 Senior Developer iBeacon on industrial Production at Fraunhofer test plant
2. 2014 Senior Developer for Dimaho mhealth Solution in Fische Fiware Accelerator
3. 2014 Senior Developer for CoJob3D Solutrion in FABolous Fiware Accelerator
4. 2017 Senior Developer at MITASSIST Project, funded by Bmbf Germany
5. 2017 Senior Developer for Industry 4.0 best practice applications for Industry 4.0 Lighthouse project Arena2036
6. H2020-INNOSUP-2014 KATANA.
7. H2020-IOT-2016-2017 IOTCRAWLER.

Most Recent Private Contracts for R&D Projects (selected examples of +15)

1. 2012 Senior Developer for BOSCH TT Product Configurator
2. 2014 Senior Developer WAFIOS AG Location awareness system for mobile services on smart manufacturing
3. 2014 Senior Developer for DEMMELER Machining online product catalogue
4. 2016-2019 Senior Developer at BASF AG Project to increase global productivity of mobile real estate assesment
5. 2018-2019 Senior Developer for WAFIOS Machine Monitor
6. 2018-2019 Senior Developer for MEMEX industrial utility film cloud platform
7. 2018-2019 Senior Developer for asvin.io IoT cloud platform
8. 2018-2019 Senior Developer for blockchain based peer-to-peer energy applicatons at EVM AG

International Awards

1. 2014 industry 4.0 solutions rated to the top 30 in Europe by 3D accelerator FABulous
2. 2014 selected as top 30 European Startup Company by European Investors Gate (EIG)
3. 2014 wearable solution selected as top 40 ehealth solution in Europe by fiche Accelerator
4. 2016 Excellence Industrie 4.0 Award by Alliance 4.0 for mobile industrial content awareness applications
5. 2018 Selected Blockchain IoT Solution Provider by Dubai Future Accelerator Cohort 5
6. 2019 2nd. Prize Award b2b Accelerator for Blockchain based IoT Security with asvin.io
7. 2019 Special Jury Award with asvin.io at Tokio FIBC (Financial Innovation Business Conference)

6.6 References

- ⁱ Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and
- ⁱⁱ <https://eugdpr.org/>
- ⁱⁱⁱ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
- ^{iv} https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01
- ^v Linder, T; Wittenstein, M; Gernandt, J; Röger, S; Industrie 4.0-Readiness. VDMA Stiftung, 2015
- ^{vi} BOOTSTRAP PROTOCOL (BOOTP) <https://tools.ietf.org/html/rfc951>
- ^{vii} Sanchez-Iborra, R.; Cano, M.D. State of the Art in LP-WAN Solutions for Industrial IoT Services. Sensors 2016, 16, 708.
- ^{viii} Minaburo, A.; Toutain, L.; Gomez, C.; Paradells, J.; Crowcroft, J. LPWAN Survey and GAP Analysis.
- ^{ix} R. Ratasuk, B. Vejlgaard, N. Mangalvedhe and A. Ghosh, "NB-IoT system for M2M communication," 2016 IEEE Wireless Communications and Networking Conference, Doha, 2016, pp. 1-5.
- ^x Sornin, N.; Luis, M.; Eirich, T.; Kramp, T.; Hersent, O. LoRaWAN Specifications; LoRaTM Alliance: Beaverton, OR, USA, 2015.
- ^{xi} Sigfox, S. SIGFOX One Network A Billion Dreams. M2M and IoT Redefined Through Cost Effective and Energy Optimized Connectivity. (White Paper) 2016.
- ^{xii} <http://www.libelium.com/development/waspmote/documentation/waspmote-lora-868mhz-915mhz-sx1272-networking-guide/>
- ^{xiii} <https://blog.temboo.com/ota-updates-for-iot/>
- ^{xiv} <https://apnsetting.com/about.html>
- ^{xv} Behcet Sarikaya, Mohit Sethi, And Dan Garcia-Carrillo. Secure IoT Bootstrapping: A Survey. Internet-Draft Draft-Sarikaya-T2trg-Sbootstrapping-06, Internet Engineering Task Force, January 2019.
- ^{xvi} InterPlanetary File System. (IPFS) <https://ipfs.io/>
- ^{xvii} Garcia-Carrillo, D., Marin-Lopez, R., Kandasamy, A., & Pelov, A. (2017). A CoAP-Based Network Access Authentication Service for Low-Power Wide Area Networks: LO-CoAP-EAP. Sensors, 17(11), 2646.
- ^{xviii} De Laat, C.; Gross, G.; Gommans, L.; Vollbrecht, J.; Spence, D. Generic AAA Architecture.
- ^{xix} Aboba, B.; Blunk, L.; Vollbrecht, J.; Carlson, J.; Levkowetz, H. Extensible Authentication Protocol (EAP). RFC 3748, 2004. <https://tools.ietf.org/search/rfc3748>
- ^{xx} Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP). RFC 7252 (Proposed Standard), 2014. Updated by RFC 7959. Available online: <https://tools.ietf.org/search/rfc7252> (accessed on 16 November 2017).
- ^{xxi} <http://www.libelium.com/development/waspmote/documentation/waspmote-lora-868mhz-915mhz-sx1272-networking-guide/>
- ^{xxii} <https://blog.temboo.com/ota-updates-for-iot/>
- ^{xxiii} <https://apnsetting.com/about.html>
- ^{xxiv} The world's leading software development platform · GitHub <https://github.com/>
- ^{xxv} Arduino Operation System <https://www.arduino.cc/>
- ^{xxvi} Contiki Operation System www.contiki-os.org/
- ^{xxvii} Linux Operation System <https://www.linux.org/>
- ^{xxviii} <https://www.forbes.com/sites/louisclumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/>
- ^{xxix} ENISA and new EU Cybersecurity Act
[http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA\(2019\)625160_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA(2019)625160_EN.pdf)
- ^{xxx} <https://arstechnica.com/information-technology/2019/04/new-variants-of-mirai-botnet-detected-targeting-more-iot-devices/>
- ^{xxxi} https://ec.europa.eu/futurium/en/system/files/ged/iop_nga_cnr_v1.0.pdf
- ^{xxxii} Trello <https://trello.com/>
- ^{xxxiii} SCRUM for Open Source Communities <https://opensource.com/resources/scrum>