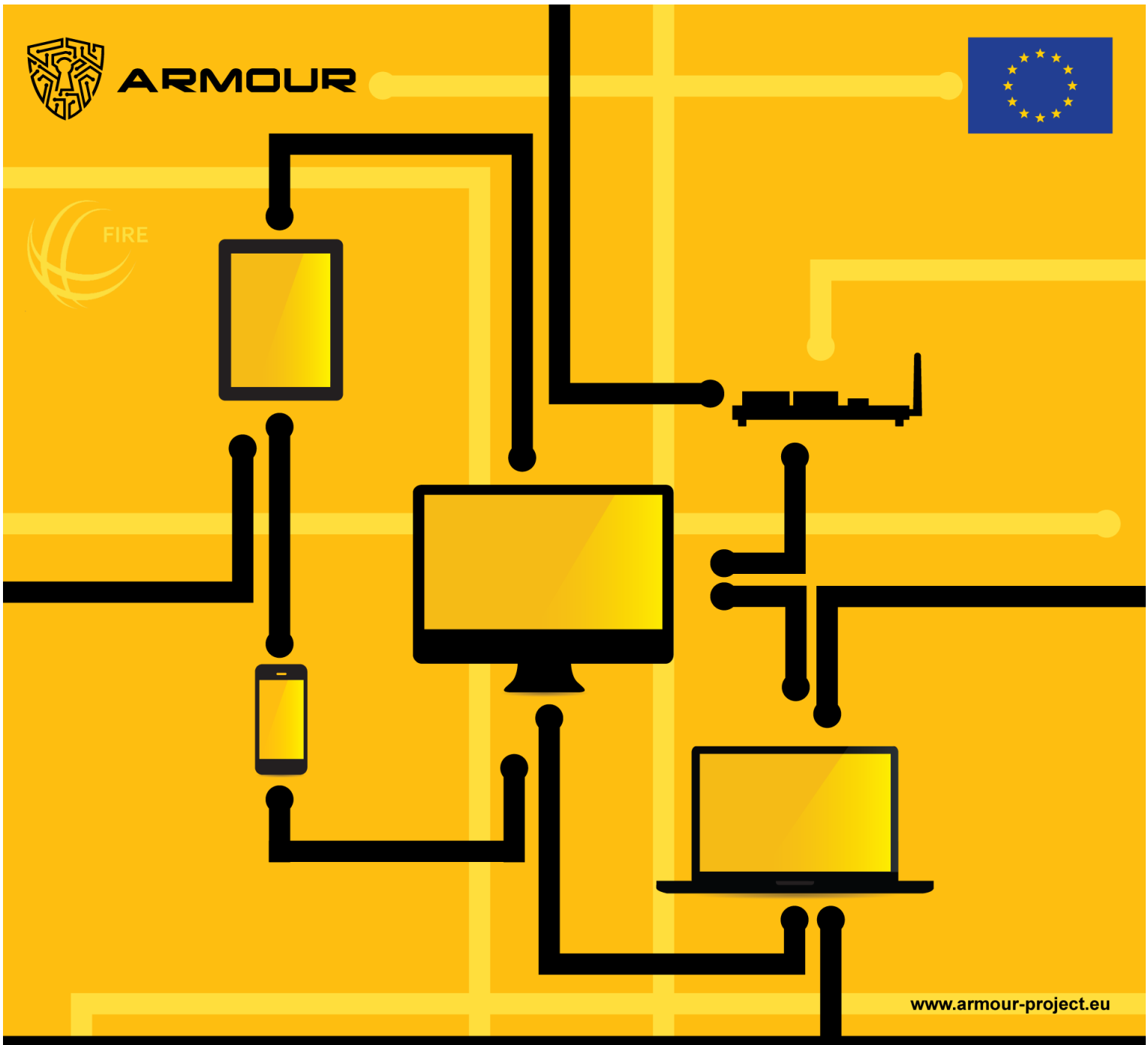
ARMOUR

FIRE



www.armour-project.eu

Deliverable D5.4

Collaboration & Clustering Activities

Version
Version 2.0

Lead Partner
Synelixis Solutions Ltd.

Date
14/04/2017

Project Name
ARMOUR – Large-Scale Experiments of IoT Security Trust

UPMC SORBONNE UNIVERSITÉS · Inria INVENTORS FOR THE DIGITAL WORLD · SYNELIXIS · Smartesting Solutions & Services · UNPARALLEL INNOVATION · European Commission · easy global market · OdinS

Call Identifier
H2020-ICT-2015

Topic
ICT-12-2015 Integrating experiments and facilities in FIRE+

Project Reference
688237

Type of Action
RIA – Research and Innovation Action

Start date of the project
February 1st, 2016

Duration
24 Months

Dissemination Level

X	**PU**	Public
	CO	Confidential, restricted under conditions set out in Model Grant Agreement
	CI	Classified, information as referred to in Commission Decision 2001/844/EC

Abstract

This deliverable describes the activities undertaken by ARMOUR partners with respect to the establishment of contacts and collaboration with relevant or complementary EU-funded and national projects, initiatives and clusters to promote project outcomes as well as receive feedback from interested stakeholders.

The main objective of this deliverable is to set the principles of the collaboration and clustering activities framework between ARMOUR and relevant european and national projects as well as initiatives that would have clear benefits towards the uptake of commercial exploitation of ARMOUR outcomes, while on the other hand, it will reveal new research opportunities for the interested partners.

It is highlighted that this document discusses the initial plan of the project with respect to clustering and collaboration activities on a european and international level. An updated version will be reported in M24 that will take into consideration the final outcomes of all the activities carried out by ARMOUR consortium, and a clear roadmap on their commercial or academic exploitation.

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688237, but this document only reflects the consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

Revision History

Revision	Date	Description	Organisation
0.1	01/12/2016	Table of Contents and assignments per partner	SYN
0.2	13/12/2016	Contributions to section 3	ODINS, SYN
0.3	28/12/2016	Contributions to section 3 and 4	SYN, ODINS, UI
0.4	29/12/2016	Contributions to section 3	UI
0.5	13/01/2017	Contributions to sections 3 and 4	EGM
0.6	15/01/2017	Contributions to section 3	UPMC
0.7	18/01/2017	Homogenization of contributions, inclusion of Abstract, Executive Summary and Conclusions.	SYN
1.0	30/01/2017	Proof-reading and minor corrections	UPMC
1.1	11/04/2017	Additional text on sections 4.1, 4.4, 4.5 addressing reviewers' comment as an outcome of M12 review	ODINS
1.2	12/04/2017	Additional text on section 4.3 addressing reviewers' comment as an outcome of M12 review	SYN
1.3	13/04/2017	Additional text on section 4.1 and section 5 addressing reviewers' comment as an outcome of M12 review	EGM
2.0	14/04/2017	Proofreading and minor corrections	UPMC

Table of Contents

1 Executive summary

This deliverable includes the ARMOUR consortium approach to Task 5.3 which deals with the establishment of contacts and collaboration with relevant EU-funded and national projects, initiatives and clusters to promote project outcomes as well as receive feedback from interested stakeholders.

The main objective of this deliverable is to set the principles of the collaboration and clustering activities framework between ARMOUR and relevant european and national projects as well as initiatives that would have clear benefits towards the uptake of commercial exploitation of ARMOUR outcomes, while on the other hand, it will reveal new research opportunities for the interested partners.

The framework described in this deliverable is based on the principles of sharing complementary experiences, expertise and exchange of best practices between ARMOUR and other projects and initiatives. The strategy will be updated on a continuous basis along the project lifetime, focusing on areas of common interest and shared commercial synergies among the consortium partners as well as other interested third parties.

Finally, this document includes the initial plan followed by the collaboration activities and participation on europe-wide initiatives and clusters until now, while an updated version will be reported in M24 that will take into consideration the outcomes of all the activities carried out by ARMOUR consortium, following the collaboration framework and clustering activities described herein.

2 ARMOUR Collaboration and Clustering Strategic Plan

Collaborative activities are fundamental towards approaching and promoting innovation. In this context, ARMOUR focuses on cooperating with and contributing to other relevant European projects and initiatives to maximize wider diffusion and effective promotion of ARMOUR outcomes to relevant stakeholders across Europe.

This deliverable details the specific plan of ARMOUR for collaboration with other EU-funded projects as well as the participation in related initatives and clusters, based on partners' expertise and specific research, industrial and/or marketing interests.

The collaboration with other EU-funded projects aims at exploiting synergies among them and thus increase their impact on the European community and market.

2.1 Plan Objectives and Strategy

In order to successfully fulfil its collaboration and clustering goals, ARMOUR has set up a comprehensive and clear plan, focusing on the following key objectives from the early stages of the project:

1. Exploitation of synergies between relevant EU-funded or national projects.
2. Promote ways to communicate the outcomes of the project in the European research community.
3. Attract relevant stakeholders from European market to promote ARMOUR framework.
4. Develop a suitable and realistic communication strategy to engage SMEs.
5. Bring together the expertise arising from different research and entrepreneurship domains.
6. Production and dissemination of common publications.
7. Collect feedback from other parties, participating in industrial fora, initiatives and clusters.
8. Pave the way towards the creation and adoption of a trust and privacy preserving framework, based on large-scale trials and open source software components that could facilitate new hardware platforms used by the European industry.

2.2 Risks associated to collaboration plan

ARMOUR consortium has performed an initial analysis concerning the barriers and risks associated to the aforementioned collaboration and clustering plan, that includes:

- Competition between partners of different project consortia or companies participating in clusters.
- Lack of information and communication channels for developments and outcomes of collaborating projects.
- Limited resources for common exploitation activities and development enhancements that could maximize impact of both projects.
- Weak connection points between industrial and research partners as well as between partners coming from both public and private sectors.
- Lack of flexibility in working practices that would prevent uptake of projects' outcomes.
- Damage to or dilution of parter's brand name by other partner's actions or delay.

- Issues arising with regard to Intellectual Property Rights if not properly addressed from the very beginning.

2.3 Foreseen mitigation measures

The possible barriers and risks described in the previous section that can potentially limit the effectiveness of the collaboration and clustering plan can be mitigated by the following measures:

- Experienced management and clear vision per collaboration activity and participation in clusters.
- Activities related to development enhancements must be based, as much as possible and where applicable, in open source concept or under clear license management.
- Partners could participate in both projects where possible, in order to have a deep and inside knowledge and thus maximize the synergies and minimize the overall coordination and communication costs.
- Mutually accepted and signed agreements and clear statements with respect to IPR, where applicable and feasible.

3 Collaboration with FIRE and H2020/NGI projects

The collaboration with other EU-funded projects will explore the possibilities for creating synergies on research, innovation and commercial dimensions, thus increasing the impact of their outcomes on European level.

The collaboration with other projects will open up new opportunities; especially those bringing new requirements, design patterns, development tools, evaluation plans, etc.

The following subsections provide a list with the projects that have been selected from ARMOUR consortium to collaborate with, after having identifying complementarities, synergies and mutual advantages.

Of course, during the project lifetime, and as ARMOUR outcomes will become more clear and mature, the list could be enhanced with other projects and collaboration activities.

3.1 FIRE infrastructures

It is obvious that ARMOUR should not only develop, capitalizing the power of FIRE services, but also influence the FIRE infrastructures and strategy. This is because ARMOUR ambitions goes beyond the concept of offering access to “raw” devices as most of the FIRE testbeds do, but most importantly aims at providing a pilot for exploring a different way to value a FIRE platform. Indeed, the idea here is to enable a service to a different research and development community by exploiting the resources provided by FIRE facilities such as Fiesta and Fit/OneLab. The service is here related to risk assessment and secured IoT solutions.

As a consequence, ARMOUR will disseminate broadly towards these two communities, namely FIRE and Security for IoT. As far as FIRE is concerned, ARMOUR is already well connected and contributes to various meetings and surveys. In addition, ARMOUR will develop synergies with F-Interop, another H2020 FIRE project with a similar approach but related to interoperability testing for IoT. Likewise, ARMOUR will develop ties and closely monitor the Fed4Fire+ flagship project of the FIRE ecosystem as we want to keep aligned with the directions and technologies adopted by Fed4Fire+.

ARMOUR consortium is also willing to cooperate with interested (commercial or academic) parties beyond Europe. For this purpose, we have adopted a dissemination plan that will be described in the relevant deliverable (D5.3). However, it is worth to mention that ARMOUR was presented both to NSF and NIST delegates. This was done **whilst Serge Fdida from UPMC was attending the IoT Forum in Washington, mid December**. A visit was carried out to NSF delegates from the CISE department in Washington HQ. **Serge Fdida met with Thyaga Nandagopal, Jack Brassil and Ken Calvert.** The main reason for the meeting was, on behalf of DG Connect, to explore potential partnership between EU and NSF on Future Wireless Platforms, somehow related to the PAWR call from NSF. However, the IoT context was mentioned as importantly relevant in the case of PAWR and the vertical developments. **The issue about security is key and was mentioned several times, highlighting the experience from and benefits arising from ARMOUR, especially with respect to a common, standardized way towards trust labeling and automated test execution for the benefit of European developers.**

Project name	Fed4Fire+
Call reference:	H2020-ICT-2016-1
Starting date:	01/01/2017
Duration:	60 months
Project website:	-

Project name	F-Interop
Call reference:	H2020-ICT-2015
Starting date:	01/11/2015
Duration:	36 months
Project website:	http://www.f-interop.eu

Likewise, ***Serge Fdida visited the NIST HQ in Gaithersborough (MA). He was hosted by Dr. Edward R. Griffor, Associate Director, SmartGrid and Cyber Physical Systems Program Office and several representatives from his team: Boynton, Paul A. (Fed) Burns, Martin (Fed) Rhee, Sokwoo (Fed) Tom Roth Wollman, David A. (Fed). The discussion was devoted to IoT standardization, interoperability and security. Awareness about ARMOUR was raised and a potential future collaboration is envisaged.***

Both actions will be continuously monitored.

ARMOUR will be an active partner of FIRE but will mostly focus on its first target group (potential users), namely IoT Security. It will take part to the discussion in this community and will showcase its experience and contributions. Likewise, ARMOUR wished to disseminate at a broader scale, thus the discussion with NSF and NIST.

3.2 H2020 & IoT/LSP projects

As already stated, ARMOUR partners have selected a set of ongoing projects to collaborate with.

It is highlighted that this list will be further enhanced during the project lifetime.

3.2.1 FORENSOR

Project name:	FOREnsic evidence gathering autonomous sensor (FORENSOR)
Call reference:	H2020-FCT-653355
Starting date:	1/9/2015
Duration:	36 Months
Project website:	http://forensor-project.eu/

FORENSOR develops and validates a novel, ultra-low-power, miniaturised, low-cost, wireless, autonomous sensor for evidence gathering, able to operate extensively without power infrastructure. FORENSOR is manageable remotely, preserves the availability and the integrity of the evidence collected, and complies with legal and ethical standards, in particular those related to privacy and personal data protection. Secure and intelligent communications let vision sensors join their forces towards robust evidence management and real time monitoring and control operations. The device combines built-in intelligence and ultra-low power consumption.

FORENSOR Wireless Visual Sensor Network inherits the characteristics of the typical WSN, in terms of capabilities and restrictions along with the support of extended wireless transmission range, the strict power restriction and rationalization and the support of adequate bandwidth to serve the transfer of the expected (relatively high) volumes of information. The network between the end devices (FORENSOR nodes) and the Server Based Application consists of two parts: (a) the low-power, low data rate wireless visual sensor network and (b) the typical TCP/IP-based wireless or wired network. These two parts are interfaced each other by the gateway.

The FORENSOR nodes are able to communicate with the (police) control centre and with each other through a secure Communications Infrastructure, which includes the nodes the gateways, and intelligent routing algorithms. The FORENSOR communication block is responsible for transferring data from the visual sensing devices to the Server Based Application (SBA), which provides the interface to the end users. The data consist of alerts, evidence and the node status (including for example the energy and storage status). Node configuration data is being sent from the SBA to the node.

Regarding the technological selections for the communications infrastructure, FORENSOR has opted for (a) the usage of sub-GHz communications with off-the-shelf hardware (SPIRIT1) from the manufacturer of the main FORENSOR board SecSoc (i.e. the project partner ST Microelectronics) and (b) the usage of networking functionality (including the RPL protocol) bundled in the Contiki Operating System. Specifically STMicroelectronics

has developed a Contiki 3.x port for the STM32 Nucleo L1 series equipped with the X-NUCLEO IDS01A expansion boards, which are sub 1GHz RF communication boards based on the SPIRIT1 transceiver.

In this perspective, FORENSOR and ARMOUR have started collaborating on the exchange of source code with regard to RPL routing and in particular aspects related to security metrics. This will allow for verifying extensions of standardized RPL routing protocol to different hardware platforms (including libraries for several commercial RF chips). Moreover, both projects, that Synelixis participates in, will benefit from importing source code into large-scale trials offered by ARMOUR FIRE infrastructures.

3.2.2 SUCCESS

Project name:	Securing Critical Energy Infrastructures (SUCCESS)
Call reference:	H2020- DRS- 700416
Starting date:	1/5/2016
Duration:	30 Months
Project website:	http://www.success-energy.eu/

SUCCESS aims at developing a new approach to the security of the energy systems, guaranteeing their security of operation, based on new concepts for Security, Resilience and Survivability, as well as Next Generation Open Real time Smart Metering, in the short and long term, and implemented as the SUCCESS Platform, supporting a complete customer-centric automation architecture, while preserving the privacy of the customers involved.

For the classification of security threats as well as mitigation techniques, SUCCESS has been based on STRIDE model. A broad description of STRIDE threat terminology and relative cryptography service under attack is shown in the next Table.

Table 1: STRIDE threat categorization

Threat	Relevant cryptography service violated	Threat Definition	Typical Victim
Spoofing	Authentication	Pretending to be something or someone legitimate entity of the system	Processes, external entities, people
Tampering	Integrity	Modifying some entry on disk, on a network, or in memory	Data stores, data flows, processes
Repudiation	Non Repudiation	Claiming that some action didn't happen, or be not responsible. Repudiation can be honest or false.	Process
Information disclosure	Confidentiality	Providing information to someone not authorized to have it	Processes, data stores, data flows
Denial of service	Availability	Absorbing resources needed to provide a service	Processes, data stores, data flows
Elevation of privilege	Authorization /Access control	Allowing someone to do something it is not authorized	Process

STRIDE is used in SUCCESS to identify vulnerabilities and enumerate different possible threats in reference with the current DFD and the assumed technologies/protocols. In the next step, attack trees are used to model and analyze attack vectors. By nature, threat modelling is the assessment of the probability, the potential harm and the addressing priority of the different attacks, which are building blocks of risk analysis and mitigation. Thus, even if these two aspects are mainly addressed in T1.3, they are also broadly discussed herein in order to end-up with a more detailed analysis that integrates any possible implications by the employed mitigation policies and relative technologies.

Through the participation of Synelixis Solutions Ltd in both projects, an in-depth discussion and opinion exchange has been performed regarding the security frameworks that have been considered for adoption within these projects. Also, although the projects are focusing on different IoT application domains with different technical requirements (one-hop versus multi-hop trees, proprietary protocols versus standardized approaches, etc), these projects share a common view with regard to the definition of a certification process. Until now, the projects are exchanging documents and views on the aforementioned subject and this collaboration is planned to continue during the next period.

3.2.3 InLife

Project name:	**INLIFE**
Call reference:	H2020- ICT-24- 732184
Starting date:	1/11/2016
Duration:	24 Months
Project website:	Not available yet.

INLIFE aims at producing, piloting, validating and demonstrating a novel, event-driven serious gamification framework for educational and social inclusion purposes, which directly links in-game progress and user experience to real-life actions and decisions, detectable through an IoT infrastructure. The central novelty of the emergent concept is that serious gaming will be directly associated to the real world. The real-life actions will be detected by processing information coming from smart environments (smart metering and smart sensors installations). Hence, the project innovation is that it creates a bridge between the emerging IoT world on one hand, and gamified virtual worlds on the other, enabling a multitude of educational, motivational and social inclusion applications.

The INLIFE architecture, depicted in Figure 1, defines two major layers, namely the IoT-based Data Adaptation Layer, which establishes communication with smart devices and takes over data aggregation and adaptation, and the Gamification Layer, which coordinates INLIFE's services provision and gamification control. In INLIFE, trainees are able to access and play Serious Games through their portable smart devices, e.g. smartphones and tablets, after they have been registered by the IoT platform. INLIFE will pilot two Serious Games developed in Unity, namely ICEBERG and AKSION, as baselines to demonstrate both overall proof of concept and platform capabilities. Nevertheless, Serious Games development is considered as an independent-external procedure, mostly devised by third parties, while the platform will provide the necessary tools and mediation framework to guarantee smooth interoperability with new applications and pilots and unrestricted access to all of its subsystems and services.

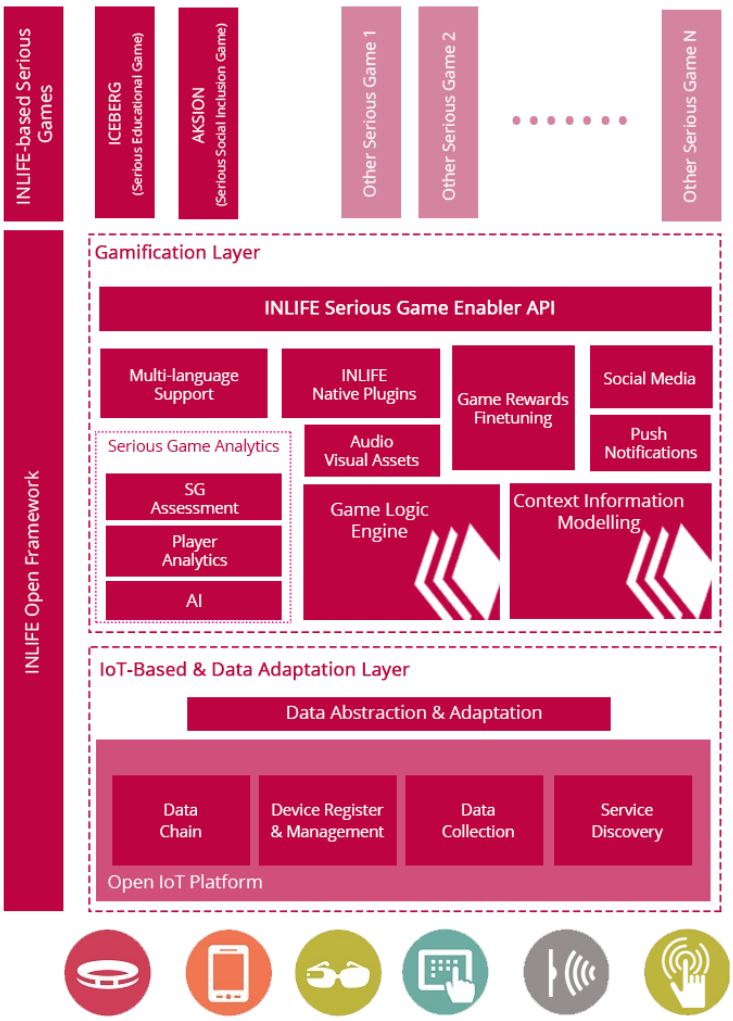


Figure 1: INLIFE platform

Data aggregation in INLIFE is built on top of an open and flexible IoT Platform, which facilitates registration, communication, data flow and smart device management providing the core IoT infrastructure and services. The IoT platform will implement both vertical and horizontal functions to support gamification Layer applications. The essence of INLIFE's IoT platform is to enable the secure connection of a multitude of heterogeneous sensing and actuating devices, having different constraints and capabilities. This includes the interaction with the hardware infrastructure, including the control of smart meters, smart plugs and sensors. Indicatively, collected information will track peoples' or objects' mobility, lighting, temperature, room occupancy, pressure forced on objects/surfaces, location/acceleration measurements, interaction with smart objects, etc. The IoT platform will provide the required scalability through its distributed message queue-based architecture for interfacing and collecting metering data from a large number of deployed meters. Also, it will employ cloudification, service discovery and sophisticated data chain technologies, in order to define credible data adaptation and flexible data management mechanisms able to enable powerful administrative tools exploited by subsystems of the Gamification Layer. INLIFE's architecture will also inherently support different communications standards (mainly IEEE-based such as WiFi and ZigBee, etc.).

One of the important tasks in INLIFE is related to security and privacy by design that will ensure that the technical system design conforms to all usual and necessary security and privacy requirements. The task will recommend the adoption and usage of secure communication protocols, secure storage mechanisms, as well as relevant anonymization and privacy preservation techniques. The corresponding specifications should define the data to be protected, as well as suitable candidate security and privacy algorithms that should be adopted (data encryption, privacy keys, digital signature, etc.). An option to enable disassociation of a player's virtual in-game identity from his/her true identity should be offered, depending on the use case; in some case, however, it might be useful for the educator to be aware of the players' identities and their performance statistics so that he/she can better address their educational needs. Furthermore, if some specific user privacy requirements are expressed by users of a serious game, then support for addressing these requirements should also be provided. Moreover, the task will specify the different roles and access rights of the framework users, together with appropriate authentication and authorization mechanisms.
Given that this project is still in the beginning, it would benefit from the threat analysis and the mitigation techniques of ARMOUR, while most importantly it could benefit from the FIRE infrastructures and the testing framework that ARMOUR is building. On the other hand, ARMOUR would benefit by testing their development (ARMOUR testing platform, specific parts of source code) on different hardware and software modules, while also dealing with requirements arising from serious games development and services. This collaboration effort is led by Synelixis that participates in both projects.

3.2.4 CREATE-IoT

Project name:	**CRoss fErtilisation through Alignment, synchronisation and Exchanges for IoT**
Call reference:	H2020-IoT-2016
Starting date:	1/1/2017
Duration:	36 Months
Project website:	Not available yet.

CREATE-IoT is a Coordination and Support Action project that aims to stimulate the collaboration between Internet of Things (IoT) initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. This requires strategic and operational synchronisation and alignment through frequent, multi-directional exchanges between the various activities under the IoT Focus Areas (FAs). It also requires cross fertilisation of the various IoT

Large Scale Pilots (LSPs) for technological and validation issues of common interest across the different application domains and use cases.

CREATE-IoT objectives are focused on reinforcing the European position in the IoT industry by supporting the IoT FA and promoting the results obtained in the LSPs. The project will perform two types of activities:

- Activities focused on contributing to align and develop synergies among the different initiatives that are already running in Europe.
- Activities aiming at helping current initiatives to expand, beyond current limits, the scope of IoT activities in strategic areas like security and art integration.

On the technical side, CREATE-IoT is mainly focused on the federation of experiments and IoT reference architectures, while the non-technical side aims at sharing experiences, assessment methodologies and business models. The knowledge collected is intended to be used for creation of a framework for an integrated European IoT Value Chain that will grow the links between communities of IoT users and providers, as well as with Member States' initiatives and other related initiatives in the IoT domain.

CREATE-IoT had its kick-off in January 2017, so no actual interaction between projects was done during the timeframe of this report. Nevertheless, it is expected that ARMOUR can collaborate with CREATE-IoT by sharing experiences collected from the execution of security experiments and by providing a testing framework and methodology. CREATE-IoT would facilitate ARMOUR outcomes and achievements to be shared and analysed by a broader audience, promoting the usage of ARMOUR tools and methodologies on diverse IoT Focus Areas and to use ARMOUR findings to help in the definition of the security dimension of the future European IoT Value Chain.

Unparallel Innovation, Lda is present in the consortia of both projects, and therefore is in a good position to facilitate the exchange of knowledge and provide access to ARMOUR technologies.

3.2.5 CPaaS.io

Project name:	**City Platform as a Service - Integrated and Open (CPaaS.io)**
Call reference:	H2020- EUJ-02-2016 IoT/Cloud/Big Data platforms in social application contexts
Starting date:	01/07/2016
Duration:	30 Months

Project website:	https://www.cpaas.io/

The main goal of this project is to develop a *City Platform as a Service* (CPaaS) that can be federated to support regional or even global applications, and that forms the basis for a smart city data infrastructure. Technical challenges that need to be addressed include data provenance, data quality, adaptive privacy levels, policies and adaptive processes for distributing and deploying processing intelligence to the cloud or to the edge. Other important aspects include data governance, data management and the empowerment of the citizen to control access and sharing of data. With respect to the latter, CPaaS.io foresees that the city-wide platform, apart from city information, will also have data about its citizens – in particular with the envisioned linking of IoT data with Open Government Data. Thus, the platform must provide all necessary security mechanisms for the desired privacy and data protection properties to materialize. However, by simply restricting all access to such data, the potential benefits for the individual as well as for the society at large of using such data are lost. CPaaS.io is therefore taking a more progressive stance using a *MyData*[1] approach: Let the citizen control who can access which personal data under what circumstances. The project will develop the necessary citizen dashboards that a citizen can not only find out what data about her is accessible through the platform, but then also can define the data access policies for other service providers. This will also enable *adaptive, context-dependent* access rules. As an example, a citizen could enable access to location and other data to rescue services during a flooding event, while in normal circumstances such data access would not be granted. Alternatively, access to personal health data would only be granted to health care providers in an emergency and rescue situation. In addition, the dashboard will enable the citizen to correct wrong data and delete unwarranted data when legally possible ("right-to-be-forgotten").

In that sense, the work that ARMOUR will offer on the security and privacy evaluation of sensors and nodes will be relevant also for CPaaS.io especially in the definition of security and privacy requirements of the platform where ARMOUR threats and security evaluation could be relevant to identify most adequate technologies and possible sensor based solutions. OdinS is leading this collaboration effort, as they participate in both projects.

3.3 FI-Core/FIWARE

Project name:	**Future Internet Core (FI-Core)**

[1] Sometimes also spelled as *midata*. Concrete and in some instances domain-specific (i.e., health care) initiatives under that name exist in the UK, Switzerland and other countries. In order not to be confused with these initiatives, we use the more generic spelling *MyData* in this proposal. A good introduction to the concept can be found in (Poikola, Kuikkaniemi and Honko 2015)

Call reference:	FP7-2013-ICT-FI
Starting date:	01/09/2014
Duration:	25 Months
Project website:	https://www.fiware.org

The FIWARE cloud and software platform is the perfect catalyst for an open ecosystem of entrepreneurs aiming at developing state-of-the-art data-driven applications. This ecosystem is formed by application developers, technology and infrastructure providers and entities that aim to leverage the impact of developing new applications based on the produced data.

Building applications based on FIWARE is intended to be quick and easy thanks to the use of pre-fabricated components in its cloud, sharing their own data as well as accessing "open" data. However, one of the challenges was to build developers' trust and confidence into this FIWARE underlying platform. This was achieved by setting up quality assurance (QA) processes relying on effective testing (Unit/Conformance/security) of the platform. This raised questions, such as balancing of test coverage with time and cost. However, several questions arise when testing IoT platforms with respect to the specificities of the communication protocols, devices and the heterogeneity of the data. Connecting "things" as devices, requires to overcome a set of problems arising in the different layers of the communication model. Using devices' produced data or responding to device's requests requires interacting with a heterogeneous and distributed environment of devices running several protocols (such as HTTP, MQTT, COAP) through multiple wireless technologies. Developers face complex scenarios where merging the information is a real challenge. For this reason, an IoT platform must enable intermediation and data gathering functions to deal with devices variety and it must be secure.

The FIWARE architecture solves the issues of heterogeneous environments where devices with different protocols are translated into to a common data format: Next Generation Service Interfaces (NGSI). FIWARE NGSI Context Management specifications are based in the NGSI Context Management specifications defined by Open Mobile Alliance (OMA). They take the form of a RESTful binding specification of the two interfaces defined in the OMA NGSI Context Management specifications, namely NGSI-9 and NGSI-10.

While several components are improving the capacities of the platform to manage stored information (security tools, advanced data store models, historical retrieval of information, linkage to third party applications, etc.), a core component known as Orion Context Broker allows to gather and manage context information between data producers and data consumers at large scale. This context broker is at the centre of the security Model Based Testing evaluation. As a matter of fact, the lack of security testing in FIWARE has been a major concern through all the development process.

In that sense, the work that ARMOUR solution will develop on the security and privacy evaluation of IoT data, transfers protocols and IoT platforms is relevant for FIWARE. Additionally, the definition of security and privacy requirements and security test cases in ARMOUR is necessary to identify vulnerabilities patterns in FIWARE.

4 Collaboration with AIOTI & IERC

This section describes the activities that took place in this period with respect to working groups in AIOTI and IERC cluster (with is now the WG1 of AIOTI). The main purpose for selecting these groups for collaboration and cooperation is that they provide unique opportunities to ARMOUR partners to grasp the most recent ideas across Europe and world-wide, meet stakeholders that would be interested in ARMOUR framework, both in terms of research as in commercial exploitation, and of course, maximize ARMOUR impact on European community.

The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015, with the aim to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT. Other objectives of the Alliance include: fostering experimentation, replication, and deployment of IoT and supporting convergence and interoperability of IoT standards; gathering evidence on market obstacles for IoT deployment; and mapping and bridging global, EU, and member states' IoT innovation activities. The legal entity maintains a close partnership with the European Commission on policy recommendations and on building the strategy for the research and innovation agenda for the future IoT funding programme and the funding members are some of the most well-known companies across Europe [1].

AIOTI maintains thirteen Working Groups of several technological, research and industrial focus, where the members of the association actively participate to.

Several groups within AIOTI are addressing aspects of IoT security and also “trust label” from different angles: WG3 from Standardisation, WG4 from policy viewpoint and WG1 (IERC) AC05 from some implementation point of view. Additionally, other groups are interested to ARMOUR partners, due to commercial interest. Details below will present the activities of the group but better synchronisation between the groups is currently in the process.

It is important to mention that the collaboration activities as well as the clustering bodies that ARMOUR participates in could evolve during the project lifetime, especially in the case that new working groups will be created.

4.1 AIOTI WG03 “standardisation”

AIoTI Working Group 03 – IoT Standardization is of relevance for ARMOUR objectives and scope and thus its work is followed by ARMOUR consortium. In particular, WG03 identifies and, where appropriate, makes recommendations to address existing IoT standards, analyses gaps in standardisation, and develops strategies and use cases aiming for: 1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, 2) semantic interoperability and 3) personal data & personal data protection to the various categories of stakeholders in the IoT space.

The “IoT Standardisation” working group (WG03) method was to start from a comprehensive IoT landscape and standardization framework [2], then to identify common High Level IoT architecture [3] and recommend how to achieve IoT Semantic interoperability [4].

Within AIOTI WG3, Philippe COUSIN from EGM is following up WG3, while Antonio Skarmeta from OdinS is mostly involved in the discussion concerning the certification of IoT and the document on Trusted IoT vision. There is also a tentative joint group discussion between the chair of this WG, EIRC AC5 and members of ARMOUR where EGM and OdinS will be involved.

Most importantly, as a tangible outcome of ARMOUR clustering and collaboration activities, a new "IoT Trust Label" task force will be created in Security sub-group, supported by ARMOUR project and lead by Philippe Cousin (EGM), followed by face-to-face meetings starting from a joint ARMOUR-AIOTI meeting, hosted by ETSI SmartM2M on 12 September 2017.

Moreover, the decisions taken within AIOTI WG03 are totally inline with ARMOUR activities. Within the AIOTI WG03 spirit and framework, the objective is to provide overview and recommendations regarding cyber-physical security and cybersecurity to the various categories of stakeholders in the various IoT ecosystems, in an IoT segmented/layered approach, both from the demand side, supply side and authorities perspective, including without limitation LSP stakeholders.

Also, WG03 decided to address security concerns in IoT architectures and ecosystems, including all layers in the applicable IoT verticals and horizontals are taken into account design and engineering principles, co-development, integration, testing, exploitation, deployment, use, monitoring security patching and end-of-life management of such IoT ecosystems.

Due to the strong interest of the consortium for the commercial exploitation of ARMOUR results, the partners will not only exploit the outcomes of the project so far, but also collaborate with interested stakeholders and collect requirements for the extension of the ARMOUR toolset.

4.2 AIOTI WG04 "policy"

This Working Group identifies, and, where appropriate, makes recommendations to address existing and potential barriers that prevent or hamper the take-up of IoT in the context of the Digital Single Market.

In October 2015, in view in supporting the coming IoT Large Scale Pilots, the WG4 issued recommendations in a report [5].

The "Policy Issues" working group (WG04) Report identifies barriers that might restrict take-up of IoT in the context of the Digital Single Market, including in relation to privacy, security and liability. The report makes recommendations to inform both the policy debate on these topics and the activities of the Large Scale Pilots.
WG4 makes the following policy recommendations:

- In relation **to privacy**, we make ten recommendations to address key concerns that have been raised in this area. These range from European Commission sponsorship of an accredited Privacy engineering program for European

educational establishments, to adoption of Privacy by Design best practice by AIOTI members.

- In relation **to security**, we make specific reference to existing industry best practices on how IoT service providers can develop IoT enabled applications, which should inform the Large Scale Pilots. We also highlight the key stakeholder, technological and societal challenges in this area, and make recommendations in respect of each.
- In respect **of liability**, WG4 considers that the rapid development of IoT technology may raise certain product compliance, product liability and insurance-related issues in the future. At present we believe that these issues can be managed within the existing legal and regulatory framework. We propose that the emphasis should, in the main, be on the development of policy solutions to these potential challenges.
- In relation to **net neutrality**, we provide a number of case studies to help inform the activities of National Regulatory Authorities across Member States in light of the finalised text on net neutrality as set out in Telecoms Single Market package.

Later in 2016, WG4 issued a new report called "AIOTI Digitisation of Industry Policy Document". In this document, the AIOTI reviews and makes a number of recommendations relevant to a number of Digitisation of Industry policy measures that are particular relevant to IoT1, namely the creation of an IoT Trust Label, IoT numbering and addressing, the 'free flow of IoT Data' and IoT liability. Wherever possible, the AIOTI includes evidence from vertical industry sectors in order to inform further discussion on these topics.

EGM is following the activities on WG4 and also encouraging more synchronisation between WG3, WG4, WG1 IERC AC05 and CPPP WG.

JRC also organised in Brussels on 6th December on «security certification».

4.3 AIOTI WG06

Working Group 06 (WG06) is one of the vertically oriented WGs within the Alliance for Internet of Things Innovation (AIOTI). The scope of AIOTI WG06 covers the scenarios and use cases where IoT-based technologies, applications and services with high added value to the actors within the plant and animal products life cycle from farm to fork.

The purpose of this Report is to provide specific recommendations on the implementation of a Large Scale Pilot (LSP) on smart farming and food safety as it is described in the IoT Focus Area call of Horizon 2020 Work Programme for 2016-2017. This LSP is expected to be an important instrument that will foster experimentation, replication and real-world deployment of IoT technologies in the European agri-food domain, while contributing to their interoperability and future market adoption.

Due to SynField product and services, Synelixis is following the work of this Working Group as it is at the core of interest for the company service portfolio.

In particular, Synelixis will be actively involved in the discussions towards the 1st AIOTI General Strategy Workshop that will take place on the 3rd and 4th of May in Toulon, France, targeting the following objectives: 1) an AIOTI strategy document which will cover the next 3 years, and 2) a strategic document per working group explaining what will be achieved, what steps will be taken and what actions need to be completed in the forthcoming period.

Participation of ARMOUR partners in these decisions, will include the promotion of the unique advantages offered by ARMOUR technological achievements, paving the way for its commercial exploitation roadmap.

4.4 IERC AC 05

The European Research Cluster on the Internet of Things has created a number of activity chains to favour close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives.

As part of collaboration with AC 05 on Trusted IoT, Odins has contributed to the presentation on Valencia EIRC meeting and the IERC AC 05 working session [6]. The vision over labelling and testing has been described and a discussion took place that highlighted issues related to the Trusted IoT vision from the report of the commission and how can be related to ARMOUR trust framework approach.

Additionally, ***OdinS has collaborated with the AC 05 as co-chairing the Workshop on User centric security, privacy and interoperability in the context of Internet of Things and Smart Cities within WF-IoT 2016 Reston VA, USA, a joint workshop between SMARTIE, RERUM and ARMOUR*** [7]. This activity has been reported as part of the annual report by the AC5 chair at AC05 Trusted IoT meeting in IERC Vienna this year.

4.5 cPPP Cybersecurity ECSO

The European Cyber Security Organisation: ECSO [8] represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders, such as large companies, SMEs and Start-ups, research centres, universities, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

ECSO is collaborating in defining the EU Cyber Security strategy and one of the areas of work of ECSO is to develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.

OdinS is participating through Antonio Skarmeta with a special interest in the work conducted in Working Group 1: Standardization Certification Labelling and Supply Chain Management, being at the core of ARMOUR interest.

As recognition of the different stakeholders present in ECSO, and the different areas of interest in the WG1 for all of them, a decision was taken to organize the working group itself with different Sub-Working-Groups (SWGs). This split intends to foster collaboration

and facilitates the achievement of the objectives. The four SWGs cover the following topics:

- **SWG 1.1. "Manufacturing of Subcomponents, Components, Devices and Products"**
  - Addressing the certification / evaluation related to simple subcomponents, such as secure IC components, up to complex products, such as cars, aircraft and others that require the integration of several components or even devices. This SWG will cover software as a product, too.
  - This SWG will focus mainly on manufacturing of cyber secure products including the respective supply-chain during integration of components.
- **SWG 1.2. "ICT infrastructure providers and other cloud based services"**
  - Addressing telecommunications or other ICT infrastructure providers, but also cloud-based ones.
  - This SWG will mainly focus of delivery of cyber secure services, but also with a significant effort on the privacy of data handling.
- **SWG 1.3. "IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management."**
  - Addressing IT Integrators and End Users (including also critical infrastructure) and the organizational and IT infrastructure changes needed to have a market of companies and suppliers able to deliver their services (ICT or non) to citizen in a secure way.
  - This SWG will mainly focus on organizations and their IT infrastructure.
- **SWG 1.4. "Base Layer"**
  - This SWG will deliver required specific capabilities to other SWGs as advanced research, definition of common terms, structures and procedures.
  - This SWG will mainly focus on having one single outcome for WG1, instead of multiple uncoordinated results.

The vision of the ECSO WG 1 is to develop this cyber security evaluation and certification system for the benefit of the protection and security of the European citizen as well as to increase the competitiveness of European industry. Thereby, considering the whole ECO-System, including not only devices and products but also the delivery of services and the continuous secure integration of devices and resulting products into larger systems.

In that sense, ARMOUR outcomes are quite relevant as product to help in the definition of the methodology and procedures that SWG1.4 need for the IoT sector. OdinS and JRC are working on defining synergies and liaison in order to work on these aspects.

Within the first WG1 meeting in Brussels Nov 17th a presentation provided by OdinS related to the ARMOUR strategy was presented and contributions from ARMOUR are expected to the initial documents.

Finally, the cPPP ECSO has initially started defining the work on the different subgroups. On WG4.1, the initial deliverable to contribute is related to the State-of-the-Art Syllabus, providing an overview of existing cybersecurity standards and certification schemes where IoT certification and labelling are going to be discussed being an initiative from ARMOUR.

5 Industry-related clustering

oneM2M is the leading global standardisation body for M2M and the IoT. The initial standardisation begun in 2008 by the different standards body partners in oneM2M.

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.

oneM2M standards initiative has a complex structure. The Steering Committee is responsible for the standard's purpose and scope. The Technical Plenary guides the high-level work on the standard thorough Work Items, which define the scope, timeline and the working group(s) responsible for it. There are 6 working groups in oneM2M responsible for different aspects of the standard, of which, the SEC and TST Working groups are of importance in ARMOUR.

The Work Item "WI-0051 Security Functions Conformance Testing" covers the security conformance testing in oneM2M and its rapporteur is Dr. Franck Le Gall from EGM. The TST working group is responsible for this WI. There are joint TST and SEC working group meetings to discuss the details about security testing because the WI covers the security features in oneM2M.

5.1 oneM2M TST WG

The oneM2M Testing WG is focusing on identifying and defining the test requirements for the oneM2M system. In addition, it develops and maintains a set of specifications for conformance and interoperability testing. As final product of this work, the WG produces test specifications in TTCN-3 language, ready for execution on different platforms. Also, the TST WG works on defining product profiles that will define which features must or should exist on the target device to be compliant with oneM2M and consequently the Test Purposes written to test these features.

As defined in ARMOUR experiments and in particular experiment 7, the MBT approach using Smartesting CertifyIt is used to generate tests for oneM2M. The model contains information that helps producing oneM2M Test Purposes. In the same time, from the model, TTCN-3 code is generated using TTCN-3 publisher for CertifyIt. The Test Purposes are contributed to the TST group. The TTCN-3 code is contributed to the oneM2M Git repository and is validated by the oneM2M Task Force.

EGM is an active contributor in the oneM2M TST WG by producing security Test Purposes based on oneM2M Security Features described in oneM2M document "TS-0003 Security Features". Also, Abbas Ahmad from EGM participated in the oneM2M Interop 2 event in Seongnam-City, South Korea, from 10 to 13 May 2016. He was involved in execution of MBT generated tests using the above approach and the oneM2MTester project on different implementations at the event.

5.1.1 oneM2MTester project

The oneM2MTester project is an independent project by multiple partners involved in oneM2M Testing WG. It aims to produce an oneM2M adapter for the Eclipse TITAN TTCN-3 compiler and executor. As an open-source project, the oneM2M community will greatly benefit from its release.

One of the results of the work in the automatization of MBT tests in ARMOUR is the contribution of new features for the MQTT and CoAP Protocol Modules to Eclipse TITAN, and those Protocol Modules are then reused in the oneM2MTester project.

5.2 oneM2M SEC WG

The oneM2M Security WG is responsible for all technical aspects regarding the security and privacy in oneM2M. Its main task is to maintain the document “TS-0003 Security Features”, but also works on additional tasks like resolving inconsistencies between TS-0001, TS-0003 and TS-0004 documents from security perspective and contributes Developer Guides for security.

Along with that, the oneM2M SEC WG collaborates with other WGs on specific issues. It collaborates with MAS WG to solve security problems from management perspective. With TST WG collaborates on security test specifications and contributing testable requirements. The security tests produced in the TST WG must be approved by both TST and SEC WGs to assure that they are correct.

The following Table presents the events to be attended by EGM representatives, their type and the expected outcome/result with respect to oneM2M activities.

Event	Dates	Type	Participant	Results
Technical Plenary TP22	14-18/03/17	Face to face (France)	N. Spaseski P. Cousin	Discussion with TST and SEC working groups engage
TST 22.3	2/05/17	online	F. Le Gall S. Cadzow	Preparing ground for launch of a security test work item
Interoperability event	9-13/05/17	Face to face (South Korea)	Ahmad	Understanding oneM2M test approach and presenting ARMOUR approach based on MBT
Technical	16-20/05/17	Face to face (South	F. Le Gall	Discussing the creation of a new Work item for

Plenary TP23		Korea)		development of security test suites with chairmen of SEC and TST working groups
TF001	10/06/16	On-line	F. Le Gall & N. Spaseski	Launch of TTCN-3 task force
TP24	18-22/07/16	Face to face (Canada)	P. Cousin	- Participating in oneM2M certification meeting to launch certification program in oneM2M - Presenting new work item (WI51) on security testing and getting it approved.
TST24.1	20/09/16	Online	N. Spaseski	Progressing WI51 & TF001
TP25	17-21/10/16	Face to face (France)	N. Spaseski P. Cousin F. Le Gall	Progressing WI51 & TF001 Discussing certification framework
TST25.2	22/11/16	Online	N. Spaseski F. Le Gall	Progressing WI51 & TF001

6 Conclusions

ARMOUR consortium strongly believes that collaboration activities among projects sharing the same scope can generate more relevant impact and higher penetration to European community.

This deliverable summarizes the activities with respect to collaboration and clustering on European level. The projects and initiatives that have been mentioned in this document have been carefully selected, after counting the relevance with ARMOUR as well as identifying clear and mutual benefits between the projects.

This deliverable introduced the collaboration plan and the activities performed during this period in order to ensure that the innovative and commercially exploitable results of ARMOUR will be disseminated to the maximum extent possible, maximizing impact.

7 References

[1] http://www.aioti.org/members/
[2] http://www.aioti.org/wp-content/uploads/2016/10/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
[3] http://www.aioti.org/wp-content/uploads/2016/10/AIOTI-WG3-IoT-High-Level-Architecture-Release_2_1.pdf
[4] https://www.researchgate.net/publication/307122744_Semantic_Interoperability_for_the_Web_of_Things?channel=doi&linkId=57c1df6008aeda1ec38cf5f5&showFulltext=true
[5] http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG04Report2015.pdf
[6] http://iot-week.eu/events/iot-week-belgrade/
[7] http://wfiot2016.ieee-wf-iot.org/program/user-centric-security-privacy-interoperability-workshop/
[8] www.ecs-org.eu