**Technical Proposal**

Summary information

|  |  |
| --- | --- |
| Approval status | Specific Agreement with EC & EFTA |
| Funding | **Maximum budget:** 414107,10**€** |
| Time scale | Mar 2018 to Feb 2020 |
| Work Items | DTR/SmartM2M-103591, TR 103 591 - DTR/SmartM2M-103533, TR 103 533 - DTR/SmartM2M-103534-1, TR 103 534-1 - DTR/SmartM2M-103534-2, TR 103 534-2 - DTR/SmartM2M-103535, TR 103 535 - DTR/SmartM2M-103536, TR 103 536 - DTR/SmartM2M-103537, TR 103 537 - DMI/SmartM2M-123141 |
| Board priority | [ETSI STF funding criteria](https://portal.etsi.org/STF/STFs/Funding.aspx) |

**Title: A coordinated approach for Security/Privacy and (Semantic) Interoperability of standardised IoT Platforms**

**Specific agreement number: ETSI/2017-08**

**Part I – Policy relevance and expected market impact**

# Policy relevance

The Internet of Things (IoT) is a key priority area of the digital single market. The IoT is an emerging technology that connects more objects to the internet - including household equipment, wearable electronics, vehicles and sensors. The number of such connected devices is expected to exceed 20 billion by 2020. Besides the innovation potential in many industrial sectors, the IoT also has the potential to help to address many societal challenges including climate change, resource and energy efficiency and ageing.

## EC Annual Union Work Programme relevance

The current technical proposal on "A coordinated approach for Security/Privacy and (Semantic) Interoperability of standardised IoT Platforms" is addressing key topics for the EC Annual Union Work Programme <http://ec.europa.eu/growth/single-market/european-standards/policy/> :

* Internet of Things,
* IoT Security and Privacy,
* IoT standardization International SDO **collaboration**,
* IoT (semantic) Interoperability (where oneM2M is recognized to be the unique global initiative and first choice for IoT/M2M interoperability framework in the ICT MSP)

This is mentioned in COM(2016) 357 final, the Communication on the annual work programme for 2017, adopted in June 2016:  
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0357&locale=en>  
As written and **highlighted** in the following extract of COM(2016) 357 final:

Section 2 on “STRATEGIC PRIORITIES FOR EUROPEAN STANDARDISATION”

Section 2.1 on “ICT Standardisation”

The Commission Communication on ICT Standardisation Priorities for the Digital Single Market identifies a list of priority building blocks for the Digital Single Market (DSM) where improved ICT standardisation is most urgent: 5G communications, cloud computing, **the internet of things (IoT),** (big) data technologies and **cybersecurity**. These are essential technology building blocks where areas such as eHealth, connected and automated vehicles, smart energy, advanced manufacturing or smart cities will rely. At this stage, the Commission does not foresee to send any standardisation requests to the ESOs but will ask for their involvement in a number of preparatory activities aiming at mapping and developing the appropriate standards. In the **internet of things (IoT)**, the Commission will **foster an interoperable environment** for the Internet of Things, working with **ESOs and international Standards Development Organisations**.

## ICT MSP RP2017 Actions relevance

The ICT MSP Rolling Plan 2017 is organized around four thematic areas: **key enablers**, societal challenges, innovation for the single market and sustainable growth.

### Internet of Things KEY ENABLER

The present technical proposal is mainly addressing the **key enabler** Internet of Things and answers to the following IoT Actions:

**ACTION 1**: Finalize the IoT standards gap analysis.

This should include an understanding of user needs, including the accessibility needs of users. Continue activities on standards landscaping and gap analysis as set up in ETSI with a specialist task force to perform these tasks, aiming to develop a set of deliverables as a reference for the LSPs: Standards landscape for IoT (who does what, what are the next milestones) and identification of potential interworking frameworks (e.g. oneM2M) Analysis of any remaining gaps to be addressed in standards to achieve the IoT vision.

**ACTION 2**: Establish some cooperation among SDOs working on standards landscaping and gap analysis in order to leverage on the results and reduce duplication of work and efforts.

**ACTION 3**: Address the semantics of standards for better data interoperability.

**ACTION 4**: High-level events — Hold thematic workshops for specific industries.

DG CNECT is following up internet standardization and maintains contacts at the highest level with key European and international SDOs that could be used to organize roundtables or other high-level involving key SDO figures, policymakers and global industry and the Commission.

### IoT Security and Privacy KEY ENABLER

This technical proposal is also addressing the following ICT MSP Rolling Plan 2017 Members’ and Stakeholders’ IoT Security and Privacy KEY ENABLER objective: *<<IoT requires the interlinking of often disparate standards. These standards are often the product of different SDOs. There is a need to bring these bodies and their standards together to achieve the often small changes needed to allow products and services to interoperate. Existing standards should be checked to take account of the protection of individuals with regard to personal data processing and the free movement of such data in the light of the proposal for a General Data Protection Regulation. Specific privacy by design standards should be identified and where necessary developed.>>*

### IoT CYBERSECURITY KEY ENABLER

The present technical proposal is also addressing the **key enabler** “CYBERSECURITY / NETWORK AND INFORMATION SECURITY” and corresponds as a response to the following Actions:

**ACTION 1:** SDOs to continue work on ensuring privacy and improving existing standards regarding the protection of individuals with regard to personal data processing.

**ACTION 2:** SDOs to develop a set of standards for critical infrastructure protection, including identification, reporting, integrity protection, and impact modelling for critical infrastructure.

**ACTION 3:** SDOs to investigate suggestions for further improvements of standards and specifications in the area of network security.

**ACTION 5:** SDOs to investigate options for collaboration to defeat and remedy attacks. No single organization has enough information to create and maintain accurate situational awareness of the threats facing itself or its users. This limitation can be overcome by sharing relevant cyberthreat information among trusted partners and communities consistent with the agreed interests of their users.

**ACTION 6:** SDOs to investigate requirements for secure protocols for networks of highly constrained devices and heavily constrained protocol interaction (low bandwidth/ultra-short session duration (50ms)/low processing capabilities).

**ACTION 8:** Create awareness of available international and global standards and frameworks on cybersecurity and promote their use and implementation

# Rationale

ETSI TC SmartM2M and oneM2M have played a key role in the success of the development and growth of the Alliance for Internet of Things Innovation (AIOTI) via the AIOTI WG03 on IoT Standardization chaired by ETSI (since 2015 and recently renewed until 2019). AIOTI is recognized as the place to ensure IoT collaboration between all key IoT stakeholders of different kinds: SDOs, Alliances, H2020 IoT funded projects (including IoT Platforms and IoT LSPs), IoT Platforms, IoT Open Sources Solutions. AIOTI does not develop IoT standards but IoT recommendations.

ETSI TC SmartM2M will cooperate with TC CYBER to address IoT Security and IoT Privacy tasks described in the current proposal. ETSI TC CYBER is a focal point on ICT Cybersecurity and has vocation to coordinate ETSI’s technical response to EU legislation related to Cybersecurity (GDPR, NIS Directive, Cybersecurity Package…). Existing TC CYBER cooperation will be leveraged in IoT Cybersecurity:

* TC CYBER cooperates with CEN/CENELEC TC 8 (privacy) and established contact with the recently created CEN/CENELEC TC 13 on "Cybersecurity and data protection" in order to ensure technical coordination between the committees.
* TC CYBER completed a major milestone with the publication of TR 103 456 “Implementation of the Network and Information Security (NIS) Directive” which provides guidance on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the legal measures and technical requirements relating to implementation of the **NIS Directive.**

ETSI TC CYBER Quantum Safe Security developments shall be incorporated in the cooperation. For example, ETSI TC CYBER (WG Quantum Safe Cryptography/QSC) published a new TR 103 570 (Quantum-Safe Key Exchanges) which compares a selection of proposals for quantum-safe key exchanges taken from the academic literature. TC CYBER WG QSC also adopted and progressed a new WI for quantum-safe VPN which will provide a review and recommendations on the impacts of integrating quantum-safe algorithms into VPN technologies.

AIOTI WG03 worked closely with the closed ETSI STF 505 on “IoT Analysis” (IoT Landscape and Gap Analysis) funded in ICT MSP RP (IoT European Large Scale Pilots (LSP) gap analysis SA/ETSI/GROW/000/2015-02) that was executed in a close collaboration with the European Commission. The same way STF 505 has been key for AIOTI and H2020 IoT LSPs, the current proposal has the ambition to play a catalyst role in the cooperation between ETSI, EC DG CONNECT (IoT Unit E4 and Cybersecurity Unit H1), ENISA, cPPP (ECSO – European Cyber Security Organisation) and all IoT stakeholders active in AIOTI. AIOTI is today the main IoT forum (lighthouse) in Europe where ETSI is WG03 (IoT Standardisation) Chairman with a world wide recognized facilitator role on IoT Standardisation collaboration and impact.

Currently, H2020 CSAs (CREATE-IoT and UNIFY-IoT where ETSI is consortium partner) are ensuring IoT Standardisation support to research and innovation on IoT Platforms and IoT LSP, the EC requested ETSI to complement H2020 CSAs and to keep the successful AIOTI and STF 505 momentum to go beyond IoT Landscaping and Gap Analysis, leveraging ICT MSP RP2017.

The ICT RP 2017, complements the AUWP and exclusively addresses ICT standardization, allows the funding of technical proposals that identify in greater detail the topic areas where IoT standards could help achieve EU Policy objectives including through complementary **interoperability testing** and **awareness actions** to ensure the effective uptake and implementation of IoT standards. ETSI has been invited to make the current technical proposal to develop IoT **recommendations** for actions including **requests for IoT standardization activities** including the development of IoT **guidelines, reports** and **supporting activities**.

The IoT Security framework of this proposal is the 13 September 2017 **Cybersecurity Package** <https://ec.europa.eu/digital-single-market/en/cyber-security> (COM(2017) 476 and 477) and the associated proposal for Regulation (Cybersecurity Agency, ENISA) and NIS directive (Directive on security of network and information systems) <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> , adopted in July 2016.

June 2017 ECSO report http://www.ecs-org.eu/working-groups/news/wg1-sota-publication on “State-of-the-Art Syllabus, Overview of existing Cybersecurity standards and certification schemes” (Cybersecurity PPP) is also a Security standards framework reference. This report has already been considered at 12 September 2017 ETSI hosted AIOTI (WG03+WG04), ENISA, ECSO, H2020 ARMOUR project and EC (DG CONNECT + DG JRC).

The IoT Privacy framework of this proposal is the next coming May 2018 GDPR (General Data Protection Regulation), REGULATION (EU) 2016/679 (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as well as the ePrivacy Directive 2002/58/EC to be replaced by coming ePrivacy Regulation.

EC DG CONNECT Unit E4 (IoT) and H1 (Cybersecurity) return of experience and feedback on former IoT Security and Privacy proposals and past actions & standardisation approaches is advising to separate now clearly IoT Security and IoT Privacy work and deliverables. There cannot effectively be any privacy with proper security and IoT Cybersecurity is most urgent than privacy (personal data protection, personal identification protection).

In the past STF505 methodology the landscaping, gap analysis and recommendations (best practises) approach can work fine to improve current IoT Cybersecurity (security, data protection) situation. There is a rationale for an urgent industry voluntary proposal for measures and actions (selections of reference standard and best practices, declaration of voluntary conformance, presumption of conformity to presume compliance with security/legislative framework (e.g. Cybersecurity Package) before next coming mandatory enforcement of any IoT security Certification (ref. 13 September EC announces/COM of Cybersecurity Package and Cyber Security Agency and 2018 regulation on Cybersecurity).

ECSO report is listing a comprehensive set of existing security standards and certification schemes (with the exception/omission of certification scheme in support of eIDAS to be added in next coming versions). The same way STF 505 helped to structure the IoT landscape, conduct a gap analysis and develop a set of recommendations on IoT architecture, interoperability and standardisation to the attention of H2020 IoT Large Scale Pilot (and other IoT testbeds), **the current proposal** shall help to refine, structure and define the selected landscape of IoT Security Standards and the level of maturity in each vertical (e.g. Smart Industry, Smart City, Smart Building, Smart Water, Smart Grid..). For example the industry sector is more advanced and mature on its voluntary & selected offer (for safety, robustness, reliability, OT – IT split, critical infrastructures support, based on the famous RAMI architecture and Industrie 4.0 selected standards). With this Smart Industry example we see that there is a need to classify (by verticals) the existing standards and their level of readiness to comply with the new Cybersecurity Package framework and its requirements regarding the degree of certification requirement.

IoT needs better IoT Security management (development, operation, maintenance, incidents management...) and to be guided in the “very” rich and diverse landscape of security standards to comply to.

The certification framework described in Cybersecurity Package is the baseline. This EC COM contains details about Security by Design and proposal to conduct voluntary initiatives of self-regulation by the industry without (in case of satisfactory self-regulation) the need for a formal legislative framework enforcement. This is a great opportunity and rationale to engage the industry in the current proposal work via AIOTI WGs, PPPs (ECSO for example for cPPP, BDVA for Big Data PPPP…) in cooperation with ENISA and EC DG CONNECT.

In it's actions towards building up EU resilience to cyber attacks the EC is inviting stakeholders to use of "security by design" methods .

*A "security by design"**approach adopted by producers of connected devices, IT software and equipment would ensure that cybersecurity is addressed before putting new products on the market. This could be part of a "duty of care" principle, to be developed together with the industry, which could reduce product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair (ref* [Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017](https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf) ) *This would also increase consumers' trust in digital products.*

This proposal, if accepted and started on time, is having a very good timing with the 2017 Cybersecurity Package plan.

Concerning IoT Privacy, the timeline and approach is different. For sure when IoT Security and Data Protection will be improved, protection of some personal data (and identification data) will be more manageable, but GDPR, ePrivacy Regulation shall enter in force in May 2018 and require more than security of data for a better privacy protection. For sure, improvement of IoT Security is a first possible good response. In the human-machine relation, privacy breach can be assessed using a Privacy Impact Assessment (PIA) that can be based on a published methodology/standard, like done in the past with RFID Mandate & Security by design work done Ref. “Recommendation On RFID Privacy Data Protection And Security & PIA” (RFID Logo, RFID PIA..). For IoT involving massive amount of data and traffic managed Human-to-machine, machine-to-machine and in complex cyber-virtual scenarii, the “privacy breach” identification need a different-than RFID “PIA” approach to study. This is more the “privacy features/characteristics” of applications’ design, providers’ application/services engagement on the “privacy by design” (insurance/guaranty) that is at stake. Classical approach of landscaping, gap analysis and recommendations published in standards should be reconsidered in a study/analysis work. For example, the study/analysis of IoT application/services providers’ approach on privacy is needed to see if there are any privacy breach evaluations. In this domain it is not only a standardisation approach but a more general analysis of the IoT privacy approach (protection measures of personal data processing) in the context of the EU legislative framework (Cybersecurity Package, NIS Directive, ePrivacy Directive, GDPR..) and European privacy value in a context of globalization of Cyber services.

The proposal shall discover how existing solutions on the market and/or technical standards could help to presume compliance to Privacy Directives, and eventually propose the creation of required standards. In addition to identification of technical standard based solutions, the proposal will identify the standard based solutions gaps like for example the technical recommendations expressed by the stakeholders that are not based on technical standards. In this case we shall report the collected positions in the report . This privacy challenges need to be analysed in a study (workshops, reports, privacy research, large scale pilots…), for example, involving AIOTI stakeholders, cPPP/ECSO with EC and ENISA in the study. The format is more in workshops organisation than TR or TS production in standardization meetings.

So the current proposal will be engaging resources to conduct this study, to engage the stakeholders and evaluate with the EC **what measures** based on standards or based on non-standard based technical characteristics of applications/services **can presume compliance with privacy directives**.

In the timeframe of the current proposal, the H2020 IoT LSP (2017-2020) will experiment IoT Security and IoT Privacy deployments. The 2018 regulation will enter in force. Like STF 505 helped AIOTI, the current proposal could facilitate AIOTI cooperation (catalyst) with H2020 IoT LSPS and other IoT Cybersecurity related funded actions.

In IERC (European IoT Research Cluster <http://www.internet-of-things-research.eu/> ), the AIOTI WG03 leaders of IoT Privacy and IoT Security sub-groups are partners of the H2020 IoT LSP CSA CREATE-IoT, this will be key to engage AIOTI and H2020 projects together. This is possible thanks to the fact ETSI is consortium partner of CREATE-IoT (and WG03 Chair) and that SmartM2M supports AIOTI WG03+WG04 (in cooperation with TC CYBER).

# Objective

The emergence of IoT ecosystems across Europe and beyond will need a solid standardized architectural framework, which offers integration of advanced IoT technologies and interoperability across IoT domains and applications, taking into account leading institutional and industry standards as well as their evolution paths. Security and Privacy as well as Semantic/Platform Interoperability have been identified.as essential key elements during a workshop entitled “IoT Standards Landscaping and Gap Analysis Workshop”, which the European Commission has organized in cooperation with the ETSI Specialist Task Force on IoT (STF 505 in February 2017).

The essential objectives of this proposed action are to build a bridge between available standards / best practices in these areas and the potential designers / implementers of such IoT ecosystems, and to support their work by providing comprehensive material for information, teaching/learning and demonstration from a more practical/industrial use perspective and for selection and implementation purposes. Furthermore they contain IoT Coordination/Collaboration support activities.

In more detail, the 3 essential objectives and envisaged corresponding deliverables of the current technical proposal are:

1. **IoT Security and Privacy**

**Privacy**

* + Analysis/study and reporting
    - Considering the privacy principles, analyse how much a better IoT Security improves IoT Privacy
    - Study how classical approach (landscaping, gap analysis, recommendations, human-to-machine PIA) based on technical standards need to be complemented by non-standard based technical measures of IoT applications/services (massive data, machine-to-machine) to comply to IoT Privacy EU framework (ePrivacy Regulation and GDPR)

Deliverable (D0): ETSI Technical Report

**Security**

* + Build a landscape of existing Security Standards (building on at least ECSO/cPPP report);
  + Identify best practices from national and European IoT initiatives/projects building on Cybersecurity Package recommendations;
  + Identify IoT Security management best practices (development, operation, maintenance, incidents management...) based on reference standards of the landscape;
  + Refine, structure and provide a selection of IoT Security Standards and their level of maturity in each IoT vertical (at least the WGs verticals of AIOTI) able to enable compliance with Cybersecurity Package and NIS Directive in order to facilitate self-declaration of conformity;

Deliverable (D1): ETSI Technical Report

**Teaching Material**

**Security**

* + Design and develop teaching materials for education on IoT Security to ensure trust in IoT and enable compliance with Cybersecurity Package and NIS Directive in order to facilitate self-declaration of conformity

Deliverable (D2-1): teaching materials on IoT Security such as an electronic textbook and a set of slides, lectures / workshops with developers and operational managers to initiate a widespread dissemination of the developed teaching materials

**Privacy**

* + Design and develop teaching materials for education on IoT Privacy
  + Guidance for understanding Compliance to IoT Privacy EU framework (ePrivacy Directives and GDPR)

Deliverable (D2-2): teaching materials on IoT Privacy such as an electronic textbook and a set of slides, lectures / workshops with developers and operational managers to initiate a widespread dissemination of the developed teaching materials

1. **IoT Semantic/Platform Interoperability**
   * Guidelines for using semantic interoperability in the industry

Deliverable (D3): ETSI Technical Report

* + Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms (e.g. AllJoyn, IoTivity, IPSO Framework, Thread), e.g. using oneM2M interworking framework, engaging SDOs and Alliances at working level based on the AIOTI HLA

Deliverable (D4): ETSI Technical Report

* + Plugtests™ event preparation on Semantic Interoperability based on AIOTI HLA, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing to demonstrate a more practical/industrial use

Deliverable (D5): ETSI Technical Report with testing organization and test scenarios

1. **IoT Coordination/Collaboration**
   * Supporting the integration and coordination among the different domains in AIOTI, to support the development of a common approach for interworking. This includes manpower for participation and remote office work in particular for AIOTI WG3.

Deliverable (D6):   
- manpower for attendance to meetings, conference calls and workshops of AIOTI  
- periodic reporting and consultation with the EC on the progress of a common coordinated approach

# Market impact

In the general context of IoT, there is a need to exchange information among different ICT systems using combination of technologies Devices (actuators, sensors, Human interfaces) have to exchange information with the different IoT systems that are present in the environment. These systems are using a wide range of communication technologies.

Even a convergence of technologies is desirable and, more strongly, it is expected in the next years, make the assumption that it will happen quickly and fully is quite unrealistic. There are huge legacies at technological and at investment levels. That will impact also future deployment for a certain numbers of years. Additionally, in the global market of IoT, will be always the need for dedicated technologies, for performance and cost reasons.

In such an environment, there is a need to find a common solution to assure at least a smooth and homogenous way to assure a very high level of interoperability (or at least interworking) among the different systems. And more relevantly, this would not be predominantly a protocol/communication technology problem, it is mainly a problem of sharing and understanding the information, achieving an interoperability at application level.

It is not an easy task, IoT is about applications, system integration and device proliferation, and this requires the capacity to integrate different objects from different business domains in a single framework. Semantic interoperability provides a very elegant manner to solve these integration problems. It is not about exchanging data, it is about sharing information.

In order to trigger those massive investments, both from the private and public sectors, a reliable and predictable standards (and regulatory) environment is needed.

The work in this proposal will lead to the identification and refinement of a common core of open interoperable standards encompassing connectivity, middleware, service layer and semantics. This include architectural frameworks, reference implementations, and full (semantic) interoperability frameworks to enable clearly defined relationships among IoT verticals.

Further developments may include working on the ontologies that will enable IoT use cases, and the requirements (knowledge) for such ontologies (knowledge representation) will need to be provided by the industry segments themselves.

**Part II – Execution of the work**

# Working method / approach

## Specialist Task Force (STF)

ETSI will perform this work by the creation of an ETSI STF, reporting the milestones to the ETSI SmartM2M Technical Committee (TC SmartM2M), according to the planned TC meeting agenda (as described in clause 7) and additional dates agreed by the TB chairman. TC SmartM2M will lead an active role in steering and contributing to this work. An STF Steering Committee (STF-SC) will be set up by TC SmartM2M in order to perform the steering task.

The STF-SC will consist of

* TC **SmartM2M** Chairman and Vice-Chairman/Chairmen,
* ETSI Secretariat **IoT Support Officer** and ETSI Funded Projects Operation (FPO),
* STF Leader (when selected),
* **European Commission** (ETSI Counsellor) representative (from DG GROW and DG CONNECT),
* ETSI Board IoT strategy group chair
* ETSI TC SmartM2M official liaison officer to the ETSI **oneM2M** Partnership Project**.**

The STF will report regularly to the STF-SC and at TC SmartM2M meetings.

The technical content described in section 7 will be developed through consultation, workshops, participation to the meetings of the projects and of AIOTI, experts’ collaboration and desk-based research. Close collaboration with the STF-SC members will be setup, as well as with the members of the main external organizations listed in section 5.2.

In particular, the STF will:

* organize periodic internal meetings of the STF to share the latest content produced
* organize periodic meetings with the STF-SC to consult on the latest advances
* attend the SmartM2M meetings and report on its activities, presenting drafts of the latest technical content produced for comments
* attend the AIOTI WG3 meetings and phone conferences
* participate to the organization of the AIOTI WG03 and SmartM2M/oneM2M workshops
* prepare contributions to the workshops and events organized by the running IoT LSPs
* invite other ETSI TCs and external SDOs to its own workshops
* organize reviews of its draft documents by the stakeholders described in section 5.2, in addition to the TC SmartM2M members

## Other interested actors

In addition to TC SmartM2M, it is expected that the STF will collaborate / exchange with the following organisations for its action:

* **AIOTI** (the Alliance for the Internet of Things Innovation http://www.aioti.eu) and in particular AIOTI WG3 on IoT Standardization that is chaired by ETSI and AIOTI WG4 on IoT Policy;
* **2017-2019 running H2020 IoT LSP** (the Internet of Things Large Scale Pilots): Smart Living for aging well : ACTIVAGE; Smart Farming and Food Security: IoF2020; Wearables for Smart Ecosystems: MONICA; Reference zones in EU Cities: SYNCHRONICITY and Autonomous vehicles in a connected environment: AUTOPILOT + 2 CSA CREATE-IoT and U4IoT ;
* **oneM2M** (the ETSI Partnership Project (EPP))
* Other ETSI Technical Committees such as TC CYBER, TC ITS, TC HF, EP eHEALTH, TC SmartBAN, etc.
* ENISA (NIS Directive, Cybersecurity Agency)
* PPPs like cPPP (ECSO), Big Data PPP (BDVA)…
* External Standard Development Organisations like CEN/ISO, CENELEC/IEC, ITU-T SG20, ISO/IEC JTC 1 SC41 and SC 27, IEEE, IETF, GS1, OASIS, OGC, 3GPP, W3C...
* National initiatives and administrations when relevant

Collaboration with stakeholders from AIOTI is of major importance as the STF is expected to exchange information and results on a regular basis with the alliance members, in particular with the WG03 which addresses standardization (see section 7 for further details). Obvious candidates as external stakeholders are also the members of the oneM2M partnership as well as the current market leaders contributing to these two organizations. The STF members will also invite players that have not been involved to date in order to fully address the markets covered.

## Expertise required (qualifications, experience, required, mix of skills)

The STF will be selected and recruited following the agreed ETSI procedures and in compliance with the terms and conditions of the Framework Partnership Agreement (FPA) signed on 26th June 2014 between the EC and ETSI as amended by Amendment 1 dated the 6th August 2015. The ETSI STF will be recruited following the issuing of an ETSI Collective Letter and this will also be available from the ETSI STF page on the ETSI Portal via the ETSI website.

Considering the above process for selecting the expertise required to perform the work described in this proposal, it is not possible at this stage to specify the individual profiles that will be recruited, however the STF will need to possess the following mix of skills and expertise:

* Technical expertise/experience with IoT and M2M in the telecom/ICT world used to work with stakeholders listed above.
* Expertise in standardisation (consensus building, technical diplomacy) of IoT/M2M (technical, organizational and semantic) at the international level.
* Experience in M2M/IoT application layer, security, safety, privacy, semantics, interworking, architecture and platforms is preferred (e.g. ETSI SmartM2M, oneM2M).
* Knowledge about the global IoT standardisation landscape and ecosystem.
* Strong personal networking ability, communications and presentation skills.
* Leadership and project management for the STF Leader position.
* Organizational skills, strong writing and reporting skills, creativity and capacity to work in a team and commitment to deliver.

It has to be noted that we are envisaging the same "Required Skills" description as STF505 (SA/ETSI/GROW/000/2015-02) that was accepted by the EC.

So, like in past STF 505 we propose an efficient and agile approach on the call and selection of experts:

- the exact number of experts and their mix of skills will depend on the number and the skills of the applications received and will be decided when setting up the STF , but It is expected that the proposed STF will comprise up to a maximum of 6 experts including the STF Leader.

- to be efficient and to avoid too much internal coordination overhead the ideal configuration would be a leader (STF Leader) engaging a minimum of agile and motivated STF experts in parallel.

As a matter of facts, this way of describing the required expertise was already accepted by the EC for STF505 (SA/ETSI/GROW/000/2015-02) and the ETSI execution gave full satisfaction to all. Based on the EC recognized success of STF 505, we propose to use the same method of recruitment, selection of experts and execution in the current proposal with ad hoc changes on the number of experts and more skills on security, privacy and safety matching with the tasks and objectives.

## Previous work

The STF will leverage the following documents and results to execute its action:

* Reports and presentations produced by AIOTI WG3, e.g., "IoT LSP Standard Framework Concepts", “SDOs Alliances Landscape" slides, "High Level Architecture (HLA)",”IoT Semantic Interoperability”, “IoT Privacy”, etc.;
* Reports produced by AIOTI WG4 on policy positions and requirements, e.g., for privacy, security, liability and net neutrality;
* ETSI TR 103 375 "SmartM2M; IoT Standards landscape and future evolutions" and TR 103 376 "SmartM2M; IoT LSP use cases and standards gaps" produced by former STF 505;
* ETSI specifications for SAREF, e.g. ETSI TS 103 264 "SmartM2M Smart Appliances Common Ontology and oneM2M mapping", ETSI TS 103 267 "SmartM2M Smart Appliances – Communication framework", ETSI TR 103 411 "SmartM2M; Smart Appliances; SAREF extension investigation";
* Documents published by the European Commission on topics related to security and privacy in the Digital Single Market:
  + Cybersecurity Package https://ec.europa.eu/digital-single-market/en/cyber-security (COM(2017) 476 and 477)
  + NIS directive (Directive on security of network and information systems) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
  + May 2018 GDPR (General Data Protection Regulation), REGULATION (EU) 2016/679 (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data);
  + Draft ePrivacy Regulation - Proposal for a Regulation on Privacy and Electronic Communications (https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications)
* June 2017 ECSO report http://www.ecs-org.eu/working-groups/news/wg1-sota-publication on "State-of-the-Art Syllabus";
* oneM2M specifications and technical reports, e.g., TS-0003 "Security Solutions", TS-0012 "oneM2M Base Ontology", TR-0012 "oneM2M End-to-End Security and Group Authentication", TR-0016 "Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies";
* Documents published by national and European IoT initiatives/projects/platforms, as soon as they are identified as valuable inputs for the STF;
* “Semantic Interoperability for the Web of Things” (aka [Joint Whitepaper on Semantic Interoperability](http://dx.doi.org/10.13140/RG.2.2.25758.13122) by AIOTI, W3C, IEEE, oneM2M)
* Semantic Interoperability Release 2.0 (AIOTI WG03 – loT Standardisation)  
  Serrano, M., Elloumi, O.,Murdock, F. P. (Eds.), ‘Semantic Interoperability Release 2.0 (AIOTI WG03 – loT Standardisation)’, 2015. 20151016
* ETSI SmartM2M Reference Ontology and oneM2M Mapping, [TS 103 264 V2.1.1](http://www.etsi.org/deliver/etsi_ts/103200_103299/103264/01.01.01_60/ts_103264v010101p.pdf)
* ITU SG-20 TD 498 Rev.1 (GEN/20) ' Updated version of Y.SC-platform “Platform Interoperability for Smart Cities and Communities”, output of Q6/20 meeting, Geneva, 25 July - 5 August 2016'
* EDPS Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data', Giovanni Buttarelli, European Data Protection Supervisor, 20161020

# Performance indicators

## Effectiveness and efficiency

The effectiveness of the project will be measured by

* The number of presentations made on the activity, at the technical meeting and at the dissemination events, at least **23**.
* The ability of the STF to achieve the objectives within the project plan provided
* The delivery of drafts and publications on schedule
* The number of drafts for consultation : including early draft, stable draft and final draft (for approval) of each of the 7 deliverables, for a total of at least **21** consultations
* The evaluation of feedback received (e.g. on WEB site, mailing lists, etc.) as minuted in **3** SmartM2M plenary meetings reports
* The number of meetings actively participated by this project: (minimum **23)**Including at least:  
  -Participation and reporting/contribution to **8** technical meetings (TC SmartM2M, AIOTI, optionally ETSI TC Cyber and others as needed)  
  -Presentation of the results at **one** annual ETSI IoT Week event will be used to engage and disseminate (optionally as well during one ETSI Security Week annual event)  
  - Presentation of the results at **one** EC dissemination workshop (potentially co hosted with AIOTI)  
  -**10** regular project meetings  
  -**3** Steering Committee meetings
* The number of participants at the meeting and their category: including a minimum of **50** Standard experts and **100** experts from the different industrial sectors as identified in the in the ICT priority areas identified by the EU Commission (document EC COM(2016) 176 - “ICT Standardisation Priorities for the Digital Single Market”), i.e., 5G, Cloud Computing, IoT, Big Data, Cybersecurity, eHealth, Smart Energy, Intelligent Transport Systems, Connected and Automated Vehicles, Advanced Manufacturing, Smart Homes, Smart Cities, and Smart Farming.

## Technical content

Technical content of the provided deliverables (draft Technical Reports) will be evaluated by ETSI TC SmartM2M and reported a minimum of 2 times in the ETSI TC SmartM2M mailing list using the remote consensus ETSI tool to collect comments and suggestions.

## Stakeholder engagement

An analysis of the effective stakeholder representation and engagement capacity in the project will be given and measured by

* Stakeholder participation in the project
* Cooperation with other external bodies, ETSI TCs, PPPs, AIOTI and ENISA
* Liaisons to identify requirements and raise awareness on the STF deliverables

## Dissemination of results

Information will be provided on the effectiveness of activities related to the dissemination of project deliverables and efforts made to raise industry and end users awareness of the activity and project deliverables. Engaged stakeholders and STF members will make every effort to contribute to relevant conferences/workshops to disseminate the project results and receive comments on the on-going work.

Information covering the dissemination activities including the presentations given and the potential press releases will be provided in the reports.

## Impact

The ICT Rolling Plan is the result of a fruitful collaboration with major standardisation stakeholders via the Multi-Stakeholder Platform on ICT Standardisation (ICT MSP). The impact priority is given to standardisation actions **aiming at ensuring interoperability, facilitating ICT uptake in key areas**.

The current technical proposal on "A coordinated approach for Security/Privacy and (Semantic) Interoperability of standardised IoT Platforms" is effectively “*aiming at ensuring interoperability, facilitating ICT uptake in key areas*” since it includes areas that are linked to key topics for the EC Annual Union Work Programme <http://ec.europa.eu/growth/single-market/european-standards/policy/> and especially in the area of:

* Internet of Things,
* IoT Security (Cyber Security)
* IoT Privacy,
* IoT standardization International SDO **collaboration**,
* IoT (semantic) Interoperability (where oneM2M is recognized to be the unique global initiative and first choice for IoT/M2M interoperability framework in the ICT MSP)

The right stakeholders are targeted since the Rolling Plan is prepared with the involvement of the ESOs and other stakeholders represented in the ICT MSP who are part of the main targeted and engaged stakeholders.

# Work plan, milestones and deliverables

## Deliverables

**Table 1: List of deliverables and reports**

|  |  |  |
| --- | --- | --- |
| **Deliverable** | **Work Item code Standard number** | **Working title** |
| D0 | DTR/SmartM2M-103591, TR 103 591 | SmartM2M; Privacy study report; Standards Landscape and best practices |
| D1 | DTR/SmartM2M-103533, TR 103 533 | SmartM2M; Security; Standards Landscape and best practices |
| D2-1 | DTR/SmartM2M-103534-1, TR 103 534-1 | SmartM2M; Teaching material; Part 1: IoT Security; |
| D2-2 | DTR/SmartM2M-103534-2, TR 103 534-2 | SmartM2M; Teaching material; Part 2: IoT Privacy |
| D3 | DTR/SmartM2M-103535, TR 103 535 | SmartM2M; Guidelines for using semantic interoperability in the industry |
| D4 | DTR/SmartM2M-103536, TR 103 536 | SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms |
| D5 | DTR/SmartM2M-103537, TR 103 537 | SmartM2M; Plugtests™ preparation on Semantic Interoperability |
| **Other STF key documents** |  | **Working title** |
| R1 | DMI/SmartM2M-123141 | Supporting the integration and coordination among the different domains in AIOTI |
| OP | - / - | Operational Plan (incl. Work Plan) |
| R2 | - / - | Interim Report to EC/EFTA |
| R3 | - / - | Final Report to EC/EFTA |

The STF will produce the following deliverables (D0-D5 for TB approval):

* **D0: DTR/SmartM2M-103591, TR 103 591**  
  Title: SmartM2M; Privacy study report; Standards Landscape and best practices   
    
  Scope: IoT privacy analysis, study and reporting. Considering the privacy principles, analyse how much a better IoT Security improves IoT Privacy, Study how classical approach (landscaping, gap analysis, recommendations, human-to-machine PIA) based on technical standards need to be complemented by non-standard based technical measures of IoT applications/services (massive data, machine-to-machine) to comply with IoT Privacy EU framework (ePrivacy Regulation and GDPR).
* **D1: DTR/SmartM2M-103533, TR 103 533**

Title: SmartM2M; Security; Standards Landscape and best

Scope: Provide an overview of the existing Security Standards Landscape with the focus on usage in the IoT domains, collect best practices from national and European IoT initiatives/projects, and provide guidance for understanding Compliance to IoTCyber Security Package. This work is expected to be developed in close collaboration with the European Commission Internet of Things unit E4 and Cybersecurity unit H1, AIOTI WG3+WG4, ETSI TC CYBER, ENISA, ECSO and related PPPs.

* **D2-1: DTR/SmartM2M-103534-1, TR 103 534-1**

Title: SmartM2M; Teaching material; Part 1: IoT Security

Scope: Develop teaching materials on IoT Security such as an electronic textbook and a set of slides, lectures / workshops with developers and operational managers to initiate a widespread dissemination of the developed teaching materials

* **D2-2: DTR/SmartM2M-103534-2, TR 103 534-2**

Title: SmartM2M; Teaching material; Part 2: IoT Privacy

Scope: Develop teaching materials on IoT Privacy such as an electronic textbook and a set of slides, lectures / workshops with developers and operational managers to initiate a widespread dissemination of the developed teaching materials

* **D3: DTR/SmartM2M-103535, TR 103 535**

Title: SmartM2M; Guidelines for using semantic interoperability in the industry

Scope: Provide guidelines, how to use semantic interoperability in the industry based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer

* **D4: DTR/SmartM2M-103536, TR 103 536**

Title: Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms

Scope: Develop an approach on how to achieve interoperability/interworking of existing standardized IoT Platforms (e.g. AllJoyn, IoTivity, IPSO Framework, Thread), e.g. using oneM2M interworking framework. This work will include technical as well as strategic aspects and aims at engagement with SDOs and Alliances at working level based on the AIOTI HLA.

* **D5: DTR/SmartM2M-103537, TR 103 537**

Title: SmartM2M; Plugtests™ preparation on Semantic Interoperability

Scope: Define and specify the preparation of a Plugtests™ event on Semantic Interoperability based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing to demonstrate a more practical/industrial use. This work will include test requirements, configurations and test descriptions in preparation of the event. This work is expected to be developed in close collaboration with the ETSI Centre for Testing and Interoperability (CTI).

The STF will produce the following other key documents:

* **R1: DMI/SmartM2M-123141**

Title: Supporting the integration and coordination among the different domains in AIOTI

Scope: Support the integration and coordination among the different domains in AIOTI, to assist the development of a common approach for interworking. This includes man power for participation and remote office work in particular for AIOTI WG3. It is providing manpower for attendance to meetings, conference calls and workshops of AIOTI and includes periodic reporting and consultation with the EC on the progress of a common coordinated approach. All of this will be documented in a report by the STF that will correspond to the miscellaneous Work Item.

* **OP: Operational Plan (incl. Work Plan)**

Scope: The objective of the Operational Plan is to plan and manage the work of the STF in order to fulfil the objectives given in the approved STF Terms of Reference. It serves as a basis to manage the STF experts’ detailed time plan, initial task allocations, duration, face-to-face meetings or conference calls (GoToMeeting) and travels. The STF leader is responsible for conducting this Operational Plan implementation and has to continuously maintain, adjust, follow it up and update it. The Operational Plan needs approval by the STF Steering Committee

* **R2: Interim Report**

The Interim Report provides EC/EFTA with an overview of the work performed by the STF from the beginning of the activity to the date the report is produced. The report promotes the activity performed within the context of the objectives set. It provides figures and facts but also a rationale and background information for the STF achievements, working methods and technical approach. The report outlines the main difficulties and proposes corrective actions to be taken by the STF itself and/or requiring the intervention of EC/EFTA, ETSI or the reference TB. It includes latest drafts of the deliverables under the Work Items.

The Interim Report requires approval by the EC/EFTA.

* **R3: Final Report**

The Final Report will be produced after the completion of the STF activity, i.e. after the deliverables have been TB approved for publication. The Final Report provides EC/EFTA with an overview of the work performed by the STF from the beginning of the activity to the date the report is produced. The report promotes the activity performed within the context of the objective set. It provides figures and facts but also a rationale and background information for the STF achievements, working methods and technical approach. The report includes the publication versions of the deliverables (TRs) promised.

The Final Report needs approval by the EC/EFTA.

**Table 2: Schedule of deliverables**

|  |  |  |
| --- | --- | --- |
| **Deliverable** | **Document Status** | **Delivery date** |
| D0: DTR/SmartM2M-103591, (TR 103 591) | * Initial (early) draft * Stable draft * Final draft | T5 T12 T14 |
| D1: DTR/SmartM2M-103533, TR 103 533 | * Initial (early) draft * Stable draft * Final draft | T5 T12 T14 |
| D2-1: DTR/SmartM2M-103534-1, TR 103 534-1 | * Initial (early) draft * Stable draft * Final draft | T9 T15 T17 |
| D2-2: DTR/SmartM2M-103534-2, TR 103 534-2 | * Initial (early) draft * Stable draft * Final draft | T9 T15 T17 |
| D3: DTR/SmartM2M-103535, TR 103 535 | * Initial (early) draft * Stable draft * Final draft | T9 T13 T15 |
| D4: DTR/SmartM2M-103536, TR 103 536 | * Initial (early) draft * Stable draft * Final draft | T5 T12 T14 |
| D5: DTR/SmartM2M-103537, TR 103 537 | * Initial (early) draft * Stable draft * Final draft | T11 T15 T17 |
| **Other STF key documents** | **Document Status** | **Delivery date** |
| R1:  DMI/SmartM2M-123141 | - / - | T3 – T17 |
| OP: Operational Plan (incl. Working Plan) | * First draft for SC approval * Updates in case of changes | T3 T4 - T18 |
| R2: Interim Report | * Draft to ETSI * Complete to EC/EFTA | T12 T13 |
| R3: Final Report | * Draft to ETSI * Complete to EC/EFTA | T19 T20 |

## Work plan

## Table 3: Work Plan

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Month** | | | | | | | | | | | | | | | | | | | | | | |
| **Task** | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| **Task 1**: Recruit-ment of experts |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 2**: Definition of the operational plan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 3**: Security and Privacy; Standards Landscape and best practices from IoT initiatives/projects. **Task 3.1 Privacy Task 3.2 Security** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 4:** Security and Privacy; Teaching material **Task 4.1 Security Task 4.2 Privacy** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 5:** Guidelines for using semantic interoperability in the industry |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 6:** Strategic / technical approach on how to achieve interoperability/ interworking of existing standardized IoT Platforms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 7:** PlugtestsTM preparation on Semantic Interoperability |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 8:** Supporting the integration and coordination among the different domains in AIOTI |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 9:** Delivery workshop event |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Task 10:** Reports and results dissemination |  |  |  |  |  |  |  |  |  |  |  | MS **A** |  |  |  |  |  |  | MS **B** |  |  |  |  |
| **Task 11:** Completion of administrative obligations |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Table 4: Milestones**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Name** | **Details** | **Date** |
| Milestone A | Interim Report | Interim Report to the EC/EFTA | T13 (+ x) |
| Milestone B | Final Report | Final Report to the EC/EFTA | T20 (+ x) |

x: approval duration within EC/EFTA

Task 1: Recruitment of expertise

The STF will be selected and recruited following the agreed ETSI procedures and in compliance with the terms and conditions of the Framework Partnership Agreement (FPA) signed between the EC and ETSI on 26th June 2014 between the EC and ETSI as amended by Amendment 1 dated the 6th August 2015. The ETSI STF will be recruited following the issuing of an ETSI Collective Letter and this will also be available from the ETSI STF page on the ETSI Portal via the ETSI website.

It is reminded that ETSI Director-General has the responsibility for the selection of the experts in consultation with the TC SmartM2M Chairman. The ETSI Secretariat and the TC SmartM2M Chairman, possibly assisted by the STF-SC, will assess the qualifications of the candidates for the STF during the selection.

|  |  |  |  |
| --- | --- | --- | --- |
| **# expertise for the task** | **Funded Manpower (man-days)** | **Duration** | **Funded Travels** |
| not applicable | not applicable | T1-T2 | None |

Task 2: Definition of the Operational Plan

Following the expert selection, the allocation of resources provided and tasks laid down in the contract will be agreed and any necessary reference documents obtained. The technical work of the project will be initiated with the first meeting of the STF. A detailed Operational Plan will be issued in the first two weeks of the STF work and published on the STF portal page on the ETSI web site. Additional content will be published throughout the unfolding of the action on the STF portal page.

The operational plan created by the STF Leader will be approved by the STF-SC.

* The STF Leader will be delegated to manage the STF experts’ detailed time plan, initial task allocations, duration, face-to-face meetings or conference calls (GoToMeeting) and travels.
* The STF Leader will follow up, update and report (for validation and adjustment) this operational plan one time per month to STF-SC.
* The STF Leader is responsible for progress reporting, drafting and provision of draft deliverables to the EC/EFTA (Interim and Final Reports).
* The STF Leader ensures the liaisons with ETSI STF administrative groups: Funded Project Operation and Funded Projects Support.

During 15 months this operation plan implementation, follow-up and revision will be ensured mainly by the STF Leader in full cooperation with STF-SC. The main efforts of the definition of the operational plan is provided at the beginning of the project (6 man-days) and will need additional resources (11 man-days) throughout the project duration to continuously maintain, adjust, follow up and report the operational plan changes for the STF-SC.

The STF Leader will maximise the efforts to conduct this operation plan implementation, follow-up and revision remotely and will need to travel 4 times in Europe to meet and engage AIOTI/IERC and SDO stakeholders.

|  |  |  |  |
| --- | --- | --- | --- |
| **# expertise for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 1 | 17 | T3 - T18 | 4 travels in Europe for the STF Leader (e.g. Steering Committee reporting) |

Task 3: Security and Privacy; Standards Landscape and best practices

This task consists mainly in 2 separated sub tasks conducted in parallel:

* Task 3.1 on IoT privacy reported in **DTR/SmartM2M-103591 (TR 103 591)**
* Task 3.2 on IoT security reported in **DTR/SmartM2M-103533 (TR 103 533)**

**Sub-Task 3.1: IoT privacy**

**Rationale reminder**

GDPR and ePrivacy Regulation shall enter in force in May 2018 and require more than security of data for a better privacy protection. The improvement of IoT Security is a first possible good response. There is a need to go beyond human-machine relation where a privacy breach can be assessed using a Privacy Impact Assessment (PIA). IoT imply a massive amount of data and traffic managed Human-to-machine and machine-to-machine and in complex cyber-virtual scenarii. The “privacy breach” identification need a different-than RFID “PIA” approach to study. So a study/analysis of IoT application/services providers’ approach on privacy is needed to see how they evaluate and prevent privacy breach. In this domain it is not only question of a technical standardisation approach but a need for a more general analysis of the IoT privacy approach (protection measures of personal data processing). So the proposal, and this sub-task, need to discover if technical standards can be produced that could help to presume compliance to Privacy Directives. The sub-task must also study if there are non-standard based technical measures. For example there are technical marketing positioning of products not based on standards like declaration on the way machine / application / services are processing data and how this is well protected against privacy breach/disclosure of personal identification data.. This privacy challenges need to be analysed in a study (workshops, reports, privacy research, large scale pilots…), for example, involving AIOTI stakeholders, cPPP/ECSO with EC and ENISA in the study. The format is more in workshops organisation than only Technical Report production in standardization meetings.

Note: human-to-machine PIA context is the “Recommendation On RFID Privacy Data Protection And Security & PIA”; <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009H0387&from=EN> ; <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf>

**Methodology**: Sub-task 3.1 consists in

* Analysing how much a better IoT Security improves IoT Privacy.
* Studying how the classical approach (landscaping, gap analysis, recommendations, human-to-machine PIA) based on technical standards need to be complemented by non-standard based technical measures of IoT applications/services (massive data, machine-to-machine) to comply to IoT Privacy EU framework (ePrivacy Regulation and GDPR)
* Collecting existing Privacy Standards with the focus on usage in the IoT domains,
  + to collect best practices from national and European IoT initiatives/projects,
  + to provide guidance for understanding Compliance to IoT Privacy EU framework (ePrivacy Regulation and GDPR)
  + and to draft it in Technical Report **DTR/SmartM2M-103591, (TR 103 591): SmartM2M; Privacy study report; Standards Landscape and best practices**.

This work is expected to be developed in close collaboration with the European Commission Cybersecurity unit E.4 and H.1, CEN-CENELEC, AIOTI WG3, oneM2M WG SEC, ETSI TC CYBER, and ECSO WG1.

**Deliverable**: Technical Report **DTR/SmartM2M-103591 (TR 103 591)**: “Privacy study report; Standards Landscape and best practices”

The report will provide the results of the task as described above.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 2 providers for Sub-Task 3.1, STF Leader and 1 STF member | 40 | T4 – T14 | 4 travels in Europe to visit European and national IoT initiatives |

**Sub-Task 3.2: IoT security**

This sub-task consists mainly in collecting existing Security Standards with the focus on usage in the IoT domains, to collect best practices from national and European IoT initiatives/projects, provide guidance for understanding Compliance to IoT Security EU framework (Cybersecurity Package, NIS Directive) and to draft it in Technical Report **DTR/SmartM2M-103533 (**TR 103 533**):** Security; Standards Landscape and best practices from IoT initiatives/projects.

**Methodology**: Collection of Security standards being relevant for application in IoT domains by organising conference calls, email communications and desktop work. This work is expected to be developed in close collaboration with the European Commission Cybersecurity unit E.4 and H.1, CEN-CENELEC, AIOTI WG3, oneM2M WG SEC, ETSI TC CYBER, and ECSO WG1.

Selection of European IoT initiatives/projects and collection of best practices concerning their application of Security standards.

Working through the IoT EU cybersecurity framework (NIS directive, 2017 Cybersecurity package and the 2017 action on certification).

The topic will be dealt with as an ETSI Technical Report.

Sub-Task 3.2 shall be operationally oriented and shall suggest concrete measures and means. The ECSO (cPPP) report shall be taken into account. The proposal shall go beyond the traditional landscaping and dig into the practical aspects of security by design of IoT systems.

**Deliverable**: Technical Report DTR/SmartM2M-103533 **(**TR 103 533**)**: “Security; Standards Landscape and best practices”

The report will provide the results of the task as described above.

Given the scope for the Security standardisation, the report will be structured according to the following segments:

* Security standards
* Best practice from national and European IoT initiatives/projects
* Guidance for understanding Compliance to IoT Security EU framework

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 3 providers for Sub-Task 3.2, STF Leader and 2 STF members | 80 | T4 – T14 | 8 travels in Europe to visit European and national IoT initiatives |

Task 4: Security and Privacy; Teaching material

This tasks consist mainly in 2 separated sub tasks conducted in parallel:

* **Sub-Task 4.1** producing **DTR/SmartM2M-103534-1,** (TR 103 534-1) "SmartM2M; Teaching material; Part 1: **IoT Security**"
* **Sub-Task 4.2** producing **DTR/SmartM2M-103534-2,** (TR 103 534-2) "SmartM2M; Teaching material; Part 2: **IoT Privacy**"

Ref. STF 515; <https://portal.etsi.org/STF/stfs/STFHomePages/STF515>; Full title: “Design and Development of Teaching Materials for Education on ICT Standardisation” ;   
Start Date : 2016-05-01 -> End Date : 2018-04-30

**Sub-Task 4.1 Security**

This task aims to facilitate education on **Security** and to raise the knowledge level of **Security** related topics among developers and operational managers of applications for IoT domains by developing teaching materials and initiating a widespread dissemination of the developed teaching materials.

**Methodology**: Identify existing teaching materials and best practises in standardisation education of ICT (e.g. from ETSI STF 515) and derive from it educational requirements for the development of the planned teaching material.

Develop main teaching materials such as a set of slides and an input for an electronic textbook by taking into account the identified educational requirements and by using interim results from the parallel **Task 3.2**.

Test the developed teaching materials in a real context (e.g. guest lectures at AIOTI meetings, workshops with developers and operational managers) and to initiate a widespread dissemination of the developed teaching materials

The topic will be dealt with as an ETSI Technical Report.

**Deliverable**: Technical Report **DTR/SmartM2M-103534-1** (TR 103 534-1) "SmartM2M; Teaching material; **Part 1: IoT Security**"

The report will provide the results of the task as described above. All teaching materials resulting from this action will be made **available for free** upon demand from the ETSI web site.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 2 experts for Task 4.1, STF Leader and 1 STF member | 50 | T8 – T17 | 5 travels in Europe to meet with the experts and universities that collaborated to STF 515 and organize workshops for testing the developed teaching materials |

**Sub-Task 4.2 Privacy**

This task aims to facilitate education on **Privacy** and to raise the knowledge level of **Privacy** related topics among developers and operational managers of applications for IoT domains by developing teaching materials and initiating a widespread dissemination of the developed teaching materials.

**Methodology**: Identify existing teaching materials and best practises in standardisation education of ICT (e.g. from ETSI STF 515) and derive from it educational requirements for the development of the planned teaching material.

Develop main teaching materials such as a set of slides and an input for an electronic textbook by taking into account the identified educational requirements and by using interim results from the parallel **Task 3.1**.

Test the developed teaching materials in a real context (e.g. guest lectures at AIOTI meetings, workshops with developers and operational managers) and to initiate a widespread dissemination of the developed teaching materials

The topic will be dealt with as an ETSI Technical Report.

**Deliverable**: Technical Report **DTR/SmartM2M-103534-2** (TR 103 534-2) "SmartM2M; Teaching material; **Part 2: IoT Privacy**"

The report will provide the results of the task as described above. All teaching materials resulting from this action will be made **available for free** upon demand from the ETSI web site.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 2 experts for Task 4.2, STF Leader and 1 STF member | 50 | T8 – T17 | 5 travels in Europe to meet with the experts and universities that collaborated to STF 515 and AIOTI and organize workshops for testing the developed teaching materials |

Task 5: Guidelines for using semantic interoperability in the industry

This task consists on providing guidelines for using semantic interoperability based AIOTI High Level Architecture and relevant standards such as oneM2M base ontology and SAREF ontology, to collect guidelines from national and European IoT initiatives/projects, to produce a coherent set of guidelines per vertical domains.

This task shall also include guidance on implementation of security and privacy.

**Methodology**: Collection of relevant standards on semantic interoperability in IoT.

Selection of national and European IoT initiatives/projects and collection of recommendations and guidelines for achieving semantic interoperability.

Working through the collected set of guidelines and recommendations from both standards and IoT initiatives/project and deriving from it a coherent set of guidelines broken down into vertical domains.

The topic will be dealt with as an ETSI Technical Report.

**Deliverable**: Technical Report DTR/SmartM2M-103535 (TR 103 535): “Guidelines for using semantic interoperability in the industry”

The report will provide the results of the task as described above.

The report will be structured according to the following segments:

* Semantic interoperability standards.
* Semantic interoperability in national and European IoT initiatives/projects.
* Guidelines for semantic interoperability in the industry.
* Applications to vertical domains / Use cases.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 3 experts for Task 5, STF Leader and 2 STF members | 70 | T8 – T15 | 3 travels in Europe to other experts and/or stakeholders |

Task 6: Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms

This task consists of proposing an approach/solution to integrate existing technologies and platforms by means of a standard solution (such as oneM2M) capable to assure a smooth interoperability/interworking for IoT services, This work will be carried in a TR that starting from the analysis of potential standard solutions will document the resolution approach and will provide some use cases if integration of existing platform and technologies.

This task shall also include guidance on implementation of security and privacy.

**Methodology**: Collection and assessment of the solution/solutions available in the context of the standard “de jure”

Selection so some existing standard/proprietary open solutions, selecting few (2-3) of the most significant and exemplificative ones to be used as use cases and for potential gaps identification, if any.

Description of the approach and related high level guidelines for the suggested standard solution capable to solution to integrate existing technologies and assure a smooth interoperability/interworking for IoT services

The topic will be dealt with as an ETSI Technical Report.

**Deliverable**: Technical Report DTR/SmartM2M-103536 (TR 103 536): “Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms”

The report will provide the results of the task as described above.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 4 providers for Task 6, STF Leader and 3 STF members | 120 | T4 – T14 | 10 travels in Europe to technical meetings of IoT platform standardisation organisations |

Task 7: Plugtests™ preparation on Semantic Interoperability

This task consists on providing guidelines required for the preparation of a Plugtests™ event on semantic interoperability.

This task will include the following activities:

1. Identification of the testing requirements on the semantic interoperability standards, especially those collected in task 5 and 6.
2. Testbed architecture including test configurations
3. Specification of a set of interoperability test descriptions/scenarios, based on ETSI methodology as defined in ETSI Testing Framework TS 118 115 V2.0.0
4. Identification on the event preparation requirements like infrastructure, IT and related tools.
5. Guidelines on requirements for anonymous reporting of the Plugtests™ outputs.

The organisation (logistics/administration) and the conduction of the event including the support to participants, are outside the scope of this proposal.

**Methodology**:

The topic will be dealt with as an ETSI Technical Report.

**Deliverable**: Technical Report DTR/SmartM2M-103537 (TR 103 537): “Plug tests preparation on Semantic Interoperability”

The report will provide the results of the task as described above.

* Semantic interoperability standards requirements collection
* Production of a set of Interoperability test descriptions
* Guidelines/cook-book on a Plugtests™ event requirements
* Requirements on a Plugtests™ test report gathering the outcomes of the event

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 3 providers for Task 7, STF Leader and 2 STF members | 70 | T10 – T17 | 4 travels in Europe to potential Plugtests™ participants |

Task 8: Supporting the integration and coordination among the different domains in AIOTI

AIOTI (the Alliance for the Internet of Things Innovation <http://www.aioti.eu>) is today the must attend place to facilitate IoT Coordination/Collaboration between SDOs, IoT Alliances and EC IoT funded initiatives working on

* IoT Security and Privacy,
* IoT standardization,
* International SDO collaboration,
* IoT (semantic) Interoperability where oneM2M is recognized to be the unique global initiative and first choice for IoT/M2M interoperability framework in the ICT MSP

In Task 8, the present action will ensure support to AIOTI and in particular supporting directly AIOTI WG3 (Chaired by ETSI) and WG4 to ensure collaboration with:

* members of AIOTI
* 2017-2019 running H2020 IoT LSP (coordinated by H2020 CSA CREATE-IoT where ETSI is consortium member)
* members of oneM2M  (ETSI Partnership Project (EPP)) and ETSI TC SmartM2M that run the present action
* members of 3GPP (ETSI Partnership Project (EPP))
* ETSI Technical Committees such as TC CYBER, TC ITS, TC HF, EP eHEALTH, TC SmartBAN, ISG CIM, TC DECT, TC ATTM/SDMC etc..
* External Standard Development Organizations like CEN/ISO, CENELEC/IEC, ITU-T SG20, ISO/IEC JTC 1 SC41, IEEE, IETF, GS1, OASIS, OGC, W3C... in relation to AIOTI
* National initiatives and administrations when relevant

Task 8 objective is to support the integration and coordination among the different domains in AIOTI. The collaboration with AIOTI stakeholders shall be based on continuous participation and support centered in the horizontal AIOTI WG3 on IoT Standardization that is organized in 5 sub-groups (IoT Landscape, High Level Architecture, IoT Semantic Interoperability, IoT Privacy and IoT Security) and ad hoc Task Forces (past STF505 link, IoT identifiers, UNIFY-IoT link ending in 2017, CREATE-IoT link, SDO collaboration..)

**Methodology**: This technical work and AIOTI support shall be developed through consultations, workshops, participations to meetings and of AIOTI, experts’ collaboration and desk-based research.

Close collaboration with the STF-SC members will be setup, as well as with the members of the main external organizations

The Task 8 of the present action will ensure

* active attendance to AIOTI WG3 meetings and phone conferences
* participation to the organization of the AIOTI WG3 and SmartM2M/oneM2M workshops
* preparation of contributions to the workshops and events organized by the running IoT LSPs
* invitation and implication of other ETSI TCs and external SDOs to present action workshops

**Deliverable**: DMI/SmartM2M-103141: “Supporting the integration and coordination among the different domains in AIOTI”

In Task 8, the action shall contribute to AIOTI development and improvement of

* Reports (recommendations) and presentations produced by AIOTI WG3, ref. "IoT LSP Standard Framework Concepts", “SDOs Alliances Landscape" , "High Level Architecture (HLA)",”IoT Semantic Interoperability”, “IoT Privacy” and "IoT Security" published at <https://aioti-space.org/resources-new/>
* Reports produced by AIOTI WG4 on policy positions and requirements, e.g., for privacy, security, liability and net neutrality;

In Task 8, the current action shall support the development of a common approach for interworking (where the role of oneM2M is key). This includes man power for participation and remote office work in particular for AIOTI WG3.

This work shall be continuously reported in R1 (DMI/SmartM2M-123141) and the supporting of the integration and coordination among the different domains in AIOTI shall consist of

* man days (and travel) for attendance to meetings, conference calls and workshops of AIOTI,
* periodic reporting and consultation with the EC on the progress of a common coordinated approach

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| 3 providers for Task 8, STF Leader and 2 STF members | 80 | T3 – T17 | 25 travels in Europe for participation in AIOTI meetings and workshops |

Task 9: Delivery workshop event

**The “Delivery workshop event”** will be organized by the STF at the end of the project (T18). The goals of this workshop are:

* To allow the presentation of results with the highest possible support of high level officials
* To summarize the main results of the project
* To gather immediate feedback and to engage the IoT community
* To discuss possible future steps

**Methodology**: Identification of relevant contributions and stakeholders; gathering of main user requirements; summary of main results.

**Format**: 1 day joint ETSI-EC DG CONNECT workshop with presentations and moderated discussions

**Location** EC premises in Brussels (to be confirmed, otherwise in the ETSI premises)

**Date** At the end of the project (T18)

**Audience** all engaged stakeholders

Partners

* EC DG CONNECT, ETSI TC SmartM2M/oneM2M
* AIOTI
* AllJoyn, IoTivity, IPSO Framework, Thread, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| STF Leader + all STF Experts | 40 | T15-T18 | 6 travels in Europe to the delivery workshop event |

Task 10: Reports and results dissemination

During the course of the project several reports and dissemination of results from the work on the deliverables will be provided.

* The 7 TC SmartM2M draft Technical Reports that result from Task 3, 4, 5, 6 and 7 will be approved by TC SmartM2M:
  + DTR/SmartM2M-103591, (TR 103 591)  
    “Privacy study report; Standards Landscape and best practices”
  + DTR/SmartM2M–103533 (TR 103 533)  
    "Security; Standards Landscape and best practices"
  + DTR/SmartM2M–103534-1, (TR 103 534-1)  
    "Teaching material; Part 1: IoT Security"
  + DTR/SmartM2M–103534-2, (TR 103 534-2)  
    " Teaching material; Part 2: IoT Privacy"
  + DTR/SmartM2M–103535 (TR 103 535)  
    "Guidelines for using semantic interoperability in the industry "
  + DTR/SmartM2M–103536 (TR 103 536)  
    "Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms "
  + DTR/SmartM2M–103537 (TR 103 537)  
    "Plugtests™ on Semantic Interoperability "
* The work on DMI/SmartM2M-123141 “Supporting the integration and coordination among the different domains in AIOTI” includes periodic reporting and consultation with the EC on the progress of a common coordinated approach
* Progress Reports to TC SmartM2M plenary meetings, to be approved by the TC SmartM2M
* The Interim Report to EC/EFTA (T13)
* Delivery workshop event (T18), with its proceedings to be included in the final report
* The Final Report to EC/EFTA (T20)

When the five Technical Reports will be approved by ETSI TC SmartM2M, it will be made publicly available for download from the ETSI web site. The draft versions requiring public access will be provided at <http://docbox.etsi.org/SmartM2M/Open/>

The main results of the project will be presented in the “Delivery workshop event” (see also Task 9) at the end of the project (T18).

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| STF Leader + all STF Experts | 40 | T3 – T20 | 10 travels in Europe to TC SmartM2M plenary meetings and workshops to report and disseminate the work results |

Task 11: Completion of administrative obligations

The ETSI secretariat has to complete some administrative obligations in order to finalize the project.

|  |  |  |  |
| --- | --- | --- | --- |
| **# experts for the task** | **Funded Manpower (units)** | **Duration** | **Funded Travels** |
| not applicable | not applicable | T21 – T23 | None |