



ETSI Specialist Task Force 547

Security/Privacy and Interoperability of standardised IoT Platforms

Presented by: **Joachim Koss**
representing **ETSI STF547**

For: **AIOTI WG3 Plenary Meeting**

03.09.2018

Agenda

- ✔ STF 547 Introduction
- ✔ STF 547 Security & Privacy
- ✔ STF 547 Interoperability/Interworking
- ✔ STF 547 Timeline
- ✔ STF 547 Support to AIOTI





ETSI STF 547 Introduction

STF 547 – ETSI Specialist Task Force on Security/Privacy and Interoperability of standardised IoT Platforms



STF 547 (<https://portal.etsi.org/STF/STFs/STFHomePages/STF547>)

is a group of experts, funded by the European Commission under the rolling plan on ICT standardization (ICT MSP Rolling Plan 2017) supported by ETSI, commissioned to

- ✔ Provide key support to some of the European Commission policies in the domain of the Internet of Things (IoT) focussed on Security and Privacy as well as Semantic/Platform Interoperability, which have been identified as essential key elements
- ✔ Identify available standards and – as importantly - best practices in these areas
- ✔ Build a bridge for the potential designers / implementers of such IoT ecosystems
- ✔ 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
- ✔ Provide support to AIOTI and in particular directly to the horizontal WG3 in order to assist the development of a common approach for interworking

STF 547 - Experts

Team leader:

- Emmanuel Darmois, CommLedge
E-mail: emmanuel.darmois@commledge.com

Team Members:

- Arthur van der Wees, iLabs Technologies
- Dimitra Stefanatou, iLabs Technologies
- Ghada Gharbi, Sensinov
- Guido Sabatini, Digital SME
- Harm Jan Arendshorst, iLabs Technologies
- Joachim Koss, JK Consulting & Projects
- Jumoke Ogunbekun, Ex2 Management
- Khalil Drira, CNRS
- Mahdi Ben Alaya, Sensinov
- Massimo Vanetti, Digital SME
- Michelle Wetterwald, Netellany
- Scott Cadzow, Cadzow Consulting

STF 547 - Background

- ✓ Recent developments in the EC policies, e.g.
 - ✓ Cybersecurity Package
 - ✓ Coming into force of GDPR (General Data Protection Regulation)
- ✓ Actions in support of technical progress in IoT
 - ✓ IoT-EPI Task Force, UNIFY-IoT CSA
 - ✓ SAREF, SAREF extensions (and SAREF STFs)
 - ✓ AIOTI, in particular WG03 work: HLA, Gaps, Virtualisation, ...
- ✓ STF 547 provides a strong support to some of the European Commission policies in the domain of the Internet of Things
 - ✓ To some extent, the work of STF 547 can be seen as a continuation of the work of STF 505, though it takes into account a larger set of challenges

STF 547 - Objectives

- ✔ The emergence of IoT ecosystems across Europe and beyond require a solid standardized architectural framework, offering the integration of advanced IoT technologies and fostering interoperability across IoT domains and applications, taking into account leading institutional and industry standards as well as their evolution paths
- ✔ The essential objectives are to
 - ✔ Identify available standards and – as importantly - best practices
 - ✔ Build a bridge for potential designers / implementers of IoT systems
 - ✔ Provide comprehensive material for information, teaching/learning and demonstration with a very practical usage and implementation perspective
 - ✔ Support AIOTI and in particular directly the horizontal WG3 in order to assist the development of a common approach for interworking

STF 547 - Deliverables

✓ Deliverables: Technical Reports

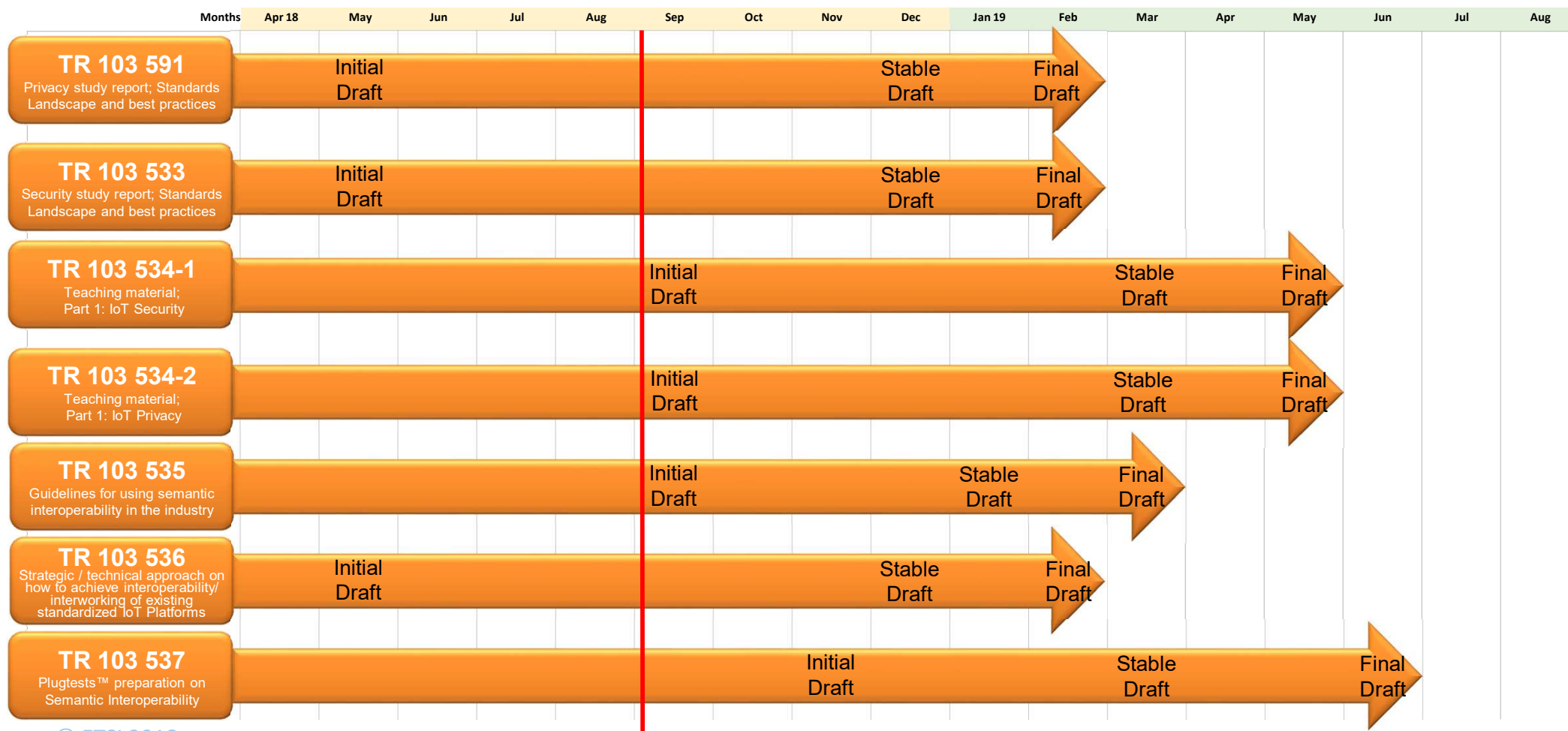
- ✓ D0 TR 103 591 Privacy; Standards Landscape and best practices
- ✓ D1 TR 103 533 Security; Standards Landscape and best practices
- ✓ D2-1 TR 103 534-1 Teaching material; Part 1: IoT Security
- ✓ D2-2 TR 103 534-2 Teaching material; Part 2: IoT Privacy
- ✓ D3 TR 103 535 Guidelines for using semantic interoperability in the industry
- ✓ D4 TR 103 536 Strategic / technical approach on how to achieve interoperability / interworking of existing standardized IoT Platforms
- ✓ D5 TR 103 537 Plugtests™ preparation on Semantic Interoperability

✓ Other deliverables

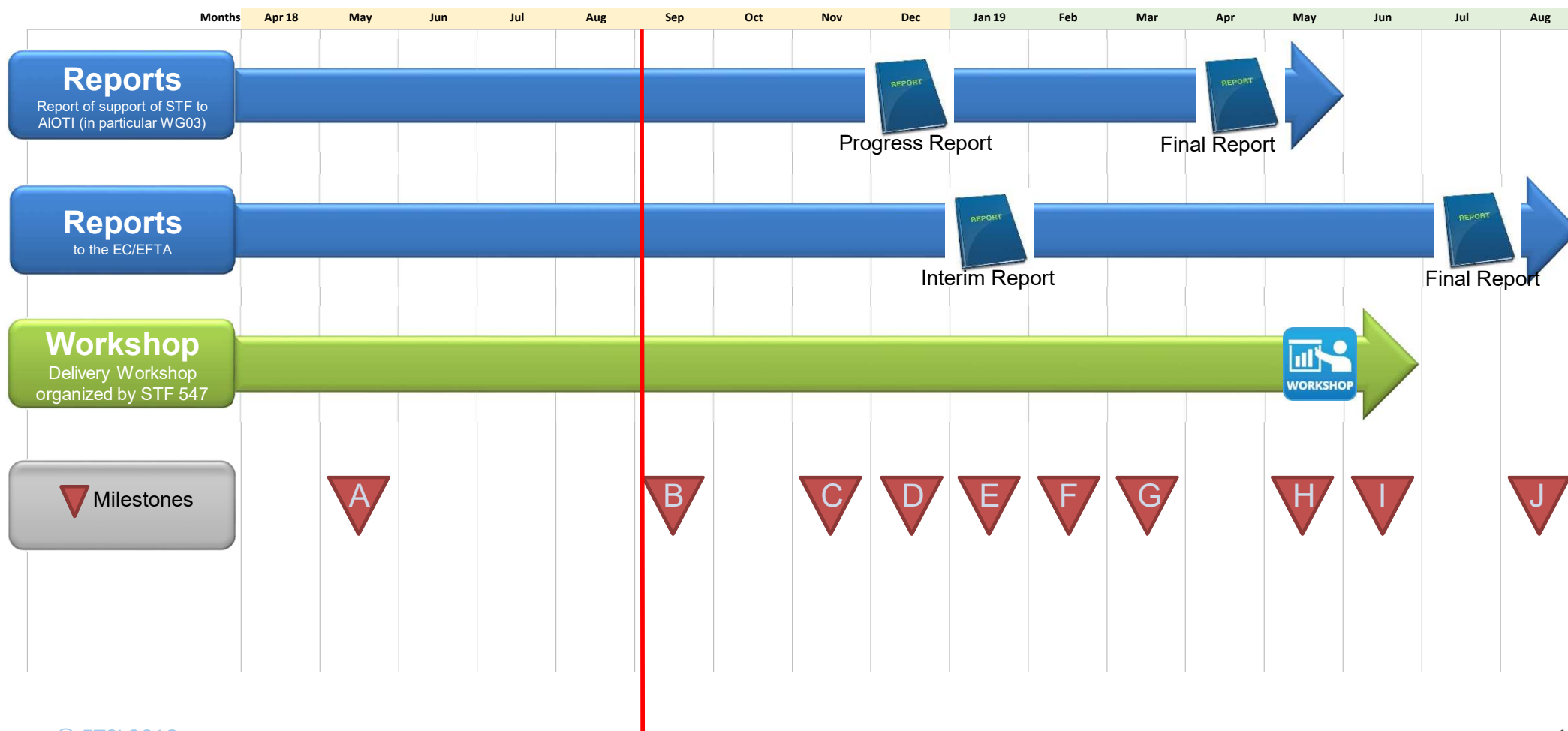
- ✓ Report of STF 547 support to AIOTI (in particular WG03)
- ✓ Delivery Workshop

ETSI Reference TC: SmartM2M

STF 547 - Work Programme (technical deliverables)



STF 547 - Work Programme (administrative deliverables)





ETSI STF 547 Security & Privacy

STF 547 - The Privacy approach

✔ Privacy

✔ Approach

- ✔ Analysing how much IoT Security improves IoT Privacy with use cases relevant for the IoT domain that will surface the necessity for a human centric approach
- ✔ Reviewing the privacy standardisation gap
- ✔ Complement the standards-based approach (landscaping, gap analysis, PIA, recommendations) by non-standard based technical measures of IoT applications & services (massive data, M2M) to comply with IoT Privacy EU framework
- ✔ Using DPIA to outline the need to emphasize on prevention rather than on detection or correction






✔ The approach adopted builds on the fundamental assumption that privacy and security are closely connected

- ✔ Security is a prerequisite for the effective protection of personal information, while further enabling the implementation of the universal SOTA Privacy Principles


✔ Development of Teaching Material in support of the approach

STF 547 - The Security approach

Security

-  Analysis of the landscape of standards and best practices in looking at IoT security requires analysis from many viewpoints: user perspective, data perspective, device perspective, resilience perspective, attacker perspective
 -  Quantify and qualify the results to guide the developers and users of IoT to select the most appropriate set of security functions in their chosen deployment
-  Mapping to the primary security development paradigms: Security by Default, Security by Design, CIA (Confidentiality, Integrity and Availability) paradigm, Design for Assurance (incorporating the Common Criteria framework)
-  Identification of best practices against each of the “normal” security paradigms further mapped to use cases for IoT and more general M2M or connected devices
-  Analysis of scenarios such as BYOD, Home IoT, and Industrial Control IoT and alignment to the use cases or scenarios developed for analysis of IoT privacy

Development of Teaching Material in support of the approach

-  Collating material from ETSI and other public sources in tutorials for various forms of media presentation (e.g. books, webinars, online course material) and building on common industry practice, e.g., the structure used in CISSP (Certified Information Systems Security Professional) development



ETSI STF 547 Interoperability/ Interworking

STF 547 - The Interoperability / Interworking approach (1)

✔ Guidelines for using Semantic Interoperability in the industry

✔ Approach

- ✔ Understand the state of the art of semantic interoperability considering recent developments from AIOTI, oneM2M, ETSI, and W3C. The focus will not be to develop a new-state-of-the-art but will rather summarize the existing efforts in terms of industry adoption
- ✔ Analyse semantic interoperability adoption by industry and investigate market inhibitors and missing issues for mass-scale deployment
- ✔ Develop guidelines about how to use semantic interoperability in the industry

✔ The development will be supported with the following actions

- ✔ Attendance and contribution to AIOTI, oneM2M and SmartM2M meetings
- ✔ Participation and contribution to LSPs project
- ✔ Consultations with research institutes and industries

STF 547 - The Interoperability / Interworking approach (2)

✔ Plugtests™ preparation on Semantic Interoperability

✔ Approach

- ✔ Identify the testing requirements on the semantic interoperability standards, especially those collected in the STF547 tasks “Guidelines for the industry” and “Interoperability of IoT Platforms”
- ✔ Define a set of related interoperability test scenarios based on results from the STF 547 tasks “Guidelines for the industry” and “Interoperability of IoT Platforms” and use case documents from e.g. AIOTI, oneM2M, SmartM2M, W3C
- ✔ Collect guidelines/cook-book on requirements for anonymous reporting of the Plugtests™ outcomes and results
- ✔ For this Plugtests™ event, the interoperability will be based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information
- ✔ Development of an ETSI Technical Report with the test scenarios and testing organization

STF 547 - The Interoperability / Interworking approach (3)

- ✔ Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms
 - ✔ Focus on one standard platform, i.e. oneM2M, and investigate its interoperability in key application domains
 - ✔ Focus on interoperability within Industrial Domain
 - ✔ Identify key references (officials of the bodies that define the standards, industry communications specialists) for the areas
 - ✔ Interoperability with devices
 - ✔ Emerging standards (e.g. OPC/UA and Internet IP)
 - ✔ Legacy standards (e.g. Modbus)
 - ✔ Interoperability with cloud frameworks
 - ✔ Investigate each of the macro-areas above in cooperation with the key references identified and define guidelines for interoperability

ETSI STF 547 Timeline

STF 547 – Main milestones

✓ Start of STF	02/03/18
✓ Final drafts of	
✓ D0 - Privacy; Standards Landscape and best practices	28/02/19
✓ D1 - Security; Standards Landscape and best practices	28/02/19
✓ D4 - Interoperability/interworking of existing standardized IoT Platforms	28/02/19
✓ D3 - Guidelines for using semantic interoperability in the industry	31/03/19
✓ D2-1 - Teaching material; Part 1: IoT Security	31/05/19
✓ D2-2 - Teaching material; Part 2: IoT Privacy	31/05/19
✓ D5 - Plugtests™ preparation on Semantic Interoperability	31/05/19
✓ Delivery Workshop (IoT Week 2019)	06/19
✓ End of STF	31/08/19



ETSI STF 547 Support to AIOTI

STF 547 – Support to AIOTI

- ✓ Supporting activities (up today, 03/09/2018)
 - ✓ WG3:
assistance in organising WG3 plenary meeting
 - ✓ WG3 – IoT relation and impact on 5G:
contribution to “IoT Relation and Impact on 5G” Release 2
 - ✓ WG3 – Semantic Interoperability:
contribution to Whitepaper Release 2
 - ✓ WG3 – IoT Landscape:
New report in AIOTI WG03 to discuss solutions on the identified IoT Gaps (ETSI STF 505)
in discussion
 - ✓ WG3 – HLA:
potential contribution **in discussion**

Contact Details

Contact Details:



Joachim Koss

JK Consulting & Projects

Email: joachim.koss@jk-conpro.de

Phone: +49 3379 379092

Mobile: +49 157 32100402

STF 547 Homepage:

<https://portal.etsi.org/STF/STFs/STFHomePages/STF547>