PROJECT FINAL PERIODIC REPORT 4
PHYLAWS - DELIVERABLE D1.4_PPR4

Grant Agreement number: 317562

Project acronym: PHYLAWS

Project title: PHYsical LAyer Wireless Security

Funding Scheme: FP7/STREP

Date of latest version of Annex I against which the assessment will be made:

Periodic report: 1st ☐ 2nd ☐ 3rd ☐ 4th X

Period covered: from July 1st, 2015 to October 30th, 2016

Name, title and organisation of the scientific representative of the project's coordinator[1]:

François Delaveau, Thales Communications & Security, France

Tel: + 33 (0)1 46 13 31 32

Fax: + 33 (0)1 41 30 33 08

E-mail: francois.delaveau@thalesgroup.com

Project website[2] address: http://www.phylaws-ict.org/

Version: 2.0

Submission date: 3/3/2017

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

Table of Content

Table of Figures

List of References

Preliminary note about the list of references below:

- When non-highlighted, the references are relevant to contracts and deliverables of period 1: Months 1 to 12.
- The yellow-highlighted references are relevant to contract's modifications and added deliverables that were achieved during to period 2: Months 13 to 32.
- The blue-highlighted references are relevant to deliverables of period 1 that were achieved during period 2: Months 13 to 32.
- The green-highlighted references are relevant to deliverables of period 2: Months 13 to 32.
- The grey-highlighted references are relevant to deliverables of period 1 and 2 that were upgraded during period 3 after PPR2 (held in Brussels 9 September 2015)
    - in order to match the recommendations of the reviewers and EC.
    - In order to updates previous analyses and results in the perspective of dissemination and standardization
- The pink-highlighted references are relevant to deliverables of period 3 (month 33-48) published during Months 32 to 40.
- The pigeon blue references are relevant to deliverables of period 3, that were published since the intermediate technical review at month 41.
- The pigeon blue underlined references are relevant to reports and deliverables of period 3 that were published after PPR4 (after Month 50).

Administrative and contract references

[PHYLAWS_GA-A] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2012-07-03, part A

[PHYLAWS_GA-DOW1] PHYLAWS Grant Agreement, referenced 317562 version V5 date 2012-07-03 (Description of Work - part B of the Grant Agreement).

[PHYLAWS_GA-WP] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2012-07-03, Work Plan

[PHYLAWS_GA-OL_PPR1] Outcome Letter of the first review ref. Ares(2014)99905 – date 2014-01-17

[PHYLAWS_GA-CR_PPR1] Consolidated Report of the first review ref. Ares(2014)99905 – date 2014-01-17

[PHYLAWS_GA-TCS_PPR1] Result of the review of our FP7/ICT project. Answer to the Outcome letter of the first review. Answer to the Consolidated Report of the first review. Ref. DCS/BRT/ASM/GG,14/076 – date 2014-02-24

[PHYLAWS_GA-AC] PHYLAWS Action Plan. Version date 2014-05-25.

[PHYLAWS_GA-DOW2] PHYLAWS Grant Agreement, referenced 317562 version V2.2 date 2014-12-19 (revised Description of Work - part B of the Grant Agreement).

[PHYLAWS_GA-WP2] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2014-12-19 (revised Work Plan).

[PHYLAWS_GA-AM1] PHYLAWS Amendment n°1 to Grant Agreement FP7-ICT-317562-PHYLAWS version date 2015-03-10.

[PHYLAWS_GA-AM2] PHYLAWS Amendment n°2 to Grant Agreement FP7-ICT-317562-PHYLAWS version date 2015-06-04.

[PHYLAWS_CA] PHYLAWS Consortium Agreement – version date 2013-11-29 signed March 2014.

[PHYLAWS_GA-OL_PPR2] Outcome Letter of the second review ref. Ares(2015)4261288 – date 2015-10-13

[PHYLAWS_GA-CR_PPR2] Consolidated Report of the second review ref. Ares(2015)4261288 – 2015-10-13

[PHYLAWS_GA-OL_PPR3] Outcome Letter of the third extra review - Ref. Ares(2016)2045260 – date 2016 – 04 – 30 - received date 2016-05-6 (by mail)

[PHYLAWS_GA-CR_PPR3] Consolidated Report of the fourth project review - Ref. Ares(2016)2045260 – date 2016 – 04 – 30 - received date 2017-02-09 (by mail).

[PHYLAWS_GA-CR_OL4] Outcome Letter of the final review - Ref. Ares(2017)6727505 – date 2017 – 02 – 07 - received date 2017-02-9 (by mail).

[PHYLAWS_GA-CR_PPR4] Consolidated Report of the final review - Ref. Ares(2017)6727505 – date 2017 – 02 – 07 - received date 2017-02-9 (by mail).

Technical and management deliverables

[PHYLAWS_KOM1] PHYLAWS Kickoff meeting 1 – version date 2013-11-14.

[PHYLAWS_KOM2] PHYLAWS Kickoff “restart” meeting 2 – version date 2015-05-22.

[PHYLAWS_ D.1.1V1_MP1] PHYLAWS management plan 1 – version V1 date 2014-3-18.

[PHYLAWS_ D.1.1V2_MP2] PHYLAWS management plan updated version V2 date 2015-06-30.

[PHYLAWS_D.1.2_PPR1] Project Periodic Report 1 – updated version V3 version date 2014-02-20.

[PHYLAWS_D.1.3] Project Periodic Report 2 – version V1.0 version date 2015-07-30.

[PHYLAWS_D.1.3_PPR2slides] Complete Slide presentation of the Project Periodic Report 2 – version V1.0 version date 2015-07-30, available on web site: https://e-ecm.online.corp.thales/livelink/livelink.exe?func=ll&objId=5636840&objAction=browse&viewType=1

[PHYLAWS_D.1.3_PPR3] Extra Project Report 3 – version V2.0 version date 2016-04-30 - version V2.1 date 2016-05-13.

[PHYLAWS_D.1.3_PPR3slides] Extra Project Report 3 (complete slide presentation) – version V1.0 date 2016-03-30 available on web site: https://e-ecm.online.corp.thales/livelink/livelink.exe?func=ll&objId=5636840&objAction=browse&viewType=1

[PHYLAWS_D.1.3_qmr1] Project quarterly month report 1 – version V1.1 version date 2016-03-15 version V2.1 date 2016-07-04

[PHYLAWS_D.1.3_qmr2] Project quarterly month report 2 – version V2.1 date 2016-07-08

[PHYLAWS_D.1.4_PPR4] Project final report 4 – version V1.0 version date 2016-12-12 – Version V2.0 version date 2017-3-3 (present document)

[PHYLAWS_D.1.4_PPR4slides] Project final report 4 (complete slide presentation) – version V1.0 date 2016-12-21, available on web site: https://e-ecm.online.corp.thales/livelink/livelink.exe?func=ll&objId=5636840&objAction=browse&viewType=1

[PHYLAWS_D.1.5] Project synthesis report – version V1.1 date 2017-2-21 - version V1.2 date 2017-3-3

[PHYLAWS_D.1.6] PHYLAWS Dissemination plan Report – version V1 date 2013-01-31.

[PHYLAWS_D.1.7] PHYLAWS Dissemination intermediate Report – version V1 date 2015-05-12

[PHYLAWS_D1.8] PHYLAWS Dissemination final report – version 1.0 date 2016-10-31.

[PHYLAWS_D.1.9] PHYLAWS Standardization plan Report – version V1 date 2013-01-31.

[PHYLAWS_D.1.10] PHYLAWS Standardization intermediate Report – version V1 date 2015-05-30

[PHYLAWS_D.1.11] PHYLAWS Standardization final report – version 1 date 2016-10-31.

[PHYLAWS_D.1.12_AB] PHYLAWS Advisory Board Meeting report – version V1 date 2013-11-08.

[PHYLAWS_D.1.13_AB] PHYLAWS Advisory Board Meeting report – version V1 date 2016-02-14.

[PHYLAWS_D1.14] PHYLAWS Advisory Board final report – version date 2016-10-31.

[PHYLAWS_D.2.1] PHYLAWS Study report "*Privacy threats for the radio interface of public wireless networks*"– revised version 2.0 date 2015-12-28.

[PHYLAWS_D.2.2] PHYLAWS Study report "*Secure architectures and protocols for privacy enhancement of radio terminals*" – version V1.0 date 2013-09-23.

[PHYLAWS_D.2.3] PHYLAWS Study report "*State of the art of physical layer security*" – version V1.1 date 2013-11-14.

[PHYLAWS_D.2.4] PHYLAWS Study report "*New opportunities provided by modern wave forms new security protocols and sensing of radio environments*" – revised version V3.0 date 2015-11-30.

[PHYLAWS_D.3.1] PHYLAWS Study report "*Channel based random generators – interm. report*" – version V1.0 date 2014-03-10.

[PHYLAWS_D.3.2] PHYLAWS Study report "*Channel based random generators – final report*" – version V2.1 date 2015-11-30.

[PHYLAWS_D.3.3] PHYLAWS Study report "*Coding techniques and algorithms for secrecy coding and secret key generation*" – version V2.0 date 2015-11-05.

[PHYLAWS_D3.4] PHYLAWS Study report "*CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band*" – version V1.0 date 2016-03-30 - version V2.0 date 2016-11-21.

[PHYLAWS_D3.5] PHYLAWS Study report "*Simulations report of PHYSEC methods using measured CIR*" – version V1.0 date 2016-12-04.

[PHYLAWS_D.4.1] PHYLAWS Study report "*TRANSEC upgrades of existing RATs - study report*" – revised version V2.0 date 2015-12-30.

[PHYLAWS_D.4.2] PHYLAWS Study report *"TRANSEC upgrades of existing RATs - simulation and analyses complements"* – version V1.0 date 2015-11-30.

[PHYLAWS_D.4.3] PHYLAWS Study report "*NETSEC upgrades of existing RATs - study report*" – version V1.0 date 2015-11-30.

[PHYLAWS_D4.4] PHYLAWS Study report "*NETSEC upgrades of existing RATs - simulation analyses complements*" – version V1.0 date 2016-08-30.

[PHYLAWS_D.4.5] PHYLAWS Study report "*New RATs and waveforms taking benefit of Physec upgrades – interim report*" – version V1.0 date 2016-10-17.

[PHYLAWS_D.4.6] PHYLAWS Study report "*New RATs and waveforms taking benefit of Physec upgrades – Final report*" – version V1.1 date 2016-11-18.

[PHYLAWS_D.5.1] PHYLAWS Study report "WiFi test bed setup development report" – version V1.0 - date 2016-03-20, version V1.1 - date 2016-04-22

[PHYLAWS_D.5.2] PHYLAWS Study report "Experiment campaign plan" – draft version V1.α - date 2016-03-24" – final version V1.0 - date 2016-04-22.

[PHYLAWS_D.5.3] PHYLAWS Study report "Intermediate Report on WiFi interceptor experiments with the test bed" – draft version V1.α – 29 / 03 / 2016 - final version V1.0 - date 2016-12-10.

[PHYLAWS_D.5.4] PHYLAWS Study *"WiFi Test bed - Final Report on WiFi Interceptor Experiments with the Test bed"* – version V1.0 - to be published

[PHYLAWS_D.5.5] PHYLAWS Study report *"Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades"* – version V1.0 - to be published

[PHYLAWS_D.6.1] PHYLAWS Study report "*Modelling of LTE-based cellular system*" – revised version V2 date 2016-02-26.

[PHYLAWS_D.6.2] PHYLAWS Study report "Simulation of interception of waveform signals in LTE-based cellular system" – version V1 Version date 2016-05-12.

[PHYLAWS_D6.3] PHYLAWS Study report "LTE-based cellular system simulations - Concluding report including simulation results and proposals for standardization", version V1.0 date 2016-09-30.

Other references

[PHYLAWS_WS] Phylaws Web site: www.phylaws-ict.org

[PHYLAWS_Patent1] Patent submitted to French office « *Procédé d'association univalente et univoque entre émetteurs et récepteurs de transmission a partir du canal de propagation*», Thales, Teknologian Tutkimuskeskus VTT, Date 29/12/2015, Number 1502713

[PHYLAWS_Patent2] Patent submitted to French office « *Procédé d'extraction univalente et univoque de clés a partir du canal de propagation* », Thales, Telecom ParisTech, Celeno Communication Ltd, Date 29/12/2015, Number 1502712

[PHYLAWS_Patent3] Patent submitted to French office « *Procédé de codage univoque et secret de transmission sur un canal de propagation à avantage de capacité*», Thales, Telecom ParisTech, Imperial College Of Science, Technology And Medicine, Date 29/12/2015, Number 1502710

[PHYLAWS_PhDTM] PhD dissertation of Mrs Taghrid Mazloum held in Telecom Paris Tech, Paris 12 Feb 2016.

List of the Partners of the Phylaws Consortium

TCS: Thales Communications and Security SAS (France)

TPT: Institut Mines Telecom – Telecom ParisTech (France)

ICL: Imperial College London (United Kingdom)

VTT: Teknologian Tutkimuskeskus (Finland)

CEL: Celeno Communications Ltd (Israel)

History of the document – evolution of its content

Redactor	Contributors Reviewers	Version	Date	Comment
François Delaveau	Renaud Molière Christiane Kameni + partners TPT CEL VTT ICL	D1.4 V1.0	14 December 2016	Report for period 4 (PPR4) and final Review Meeting 4 (RM4)
François Delaveau	Renaud Molière	D1.4 V2.0	3 March 2017	Completion of financial data. Include of parts of reviewers recommendations. Insertion of PPR4 slides. Correction of typo errors and English language. New pagination. Update of dissemination and IPR issues. Update of references

Added notes on this deliverable:

- This deliverable is a version 2.0 of the final periodic report, which deals with the overall results, management, cost issues and technical work of the PHYLAWS project during its 3rd period: from the 1st of July 2015 to the 30th of October 2016 (i.e. M33 - M 48). It includes updates of risk analyses and ethical issues. In addition it synthetizes the work done all over the Phylaws project that ends after this period.
- This document is completed by slides [PHYLAWS_D.1.4_PPR4slides] that supported the final review meeting (named RM4) of period 3 (planed 21 December 2016 in Brussels – see agenda proposal and conclusion of the review in annex 1). These slides describe the technical part of the PPR4 and contain all the details about the work achieved in technical Work Packages WP3 to WP6 (WP2 is already finished), as well as about management, dissemination and standardization efforts during the last period of the PHYLAWS project (Work Package WP1).
- Since the publication of the version V1.0 before the final review meeting of the project (RM4, planned 21st of December 2016 in Brussels), some information were added :
    - Information relevant to the late deliverables of WP5 (deliverable D5.3 final version, deliverables D5.4 and D5.5)
    - Information relevant to costs which are submitted to audits and information relevant to the completion of NEF by all partners
    - Answer and complement to the remarks of reviewers and EC expressed in their report [PHYLAWS_GA-CR_OL4] [PHYLAWS_GA-CR_PPR4].
- This document also includes overall results, management and cost issues of periods M33-M39, M41-M44 which are already covered by the intermediate technical report [PHYLAWS_D.1.3_PPR3] and [PHYLAWS_D.1.3_PPR3slides] and the Quarterly Month Reports QMR1 [PHYLAWS_D.1.3_qmr1] QMR2 [PHYLAWS_D.1.3_qmr2].
- The present version 2.0 of this final report (referenced deliverable D1.4 [PHYLAWS_D1.4PPR4]) is completed by a synthesis report (referenced deliverable D1.5 [PHYLAWS_D.1.5]) recalling all the deliverables and results of the project.

Glossary

Term	Definition
AN-BF	Artificial Noise – Beam Forming
AP	Access Point
CFR	Channel Frequency Response (of the radio-propagation filter). CFR = FFT(CIR).
CIR	Channel Impulse Response (of the radio-propagation filter). CIR = FFT^{-1}(CFR) – provided by single sense radio channel estimation
COMSEC	Communication Security: is relevant to the protection of the content of user messages (voice, data). COMSEC applies either at the radio interface or at upper layer. COMSEC techniques involve ciphering, authentication and integrity control of signalling and user data at several protocol layers and interfaces (examples are point to point ciphering of each data flux, ciphering of IP packets, ciphering of artery, etc.).
CSI	Channel State Information – provided by dual sense radio channel estimation and channel restoration capabilities (with calibration, post computing etc.) when needed and relevant.
FDD	Frequency Division Duplexing (communicating devices operate in different carrier frequencies)
IAS	Interrogation and Acknowledgment Sequences: radio protocol derived from concepts of Identification Friend or Foe Radio systems. IAS is performed by exchanging Tag Signals between legitimate transmitters and receivers, and achieve security pairing and secured estimation of radio channels.
IJ	Intelligent Jammer: Eavesdropping and jamming (protocol aware) system that jams dedicated part of the legitimate radio protocol (such as channel probes used for CSI for example).
LOS, NLOS	Line Of Sight, Non Line Of Sight
MITM	Man-in-the-Middle: Eavesdropping and spoofing system that intercepts and modifies messages within the legitimate protocol in real time.
NETSEC	Network Transmission Security: NETSEC is relevant to the protection of the signalling of the network. NETSEC applies mainly at the radio interface and at the medium access protocol layer, with request to upper protocol layers. NETSEC techniques involve mainly transmitter authentication protocols, integrity control and ciphering of signalling data.
PHYSEC	Physical Layer Security is a generic term that will be used in this project to design all kind of protection techniques that are based on the use of the physical layer sensing and/or measurement.
RAT	Radio Access Technology (e.g. FDMA, TDMA, CDMA, CSMA, OFDM, Full Duplex, SISO, SIMO, MISO, MIMO, etc.)
SC	Secrecy Coding: coding schemes ensuring low or null information leakages towards any eavesdropper location while enabling a controlled BER data transmission towards legitimate receiver. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent3]
SKG	Secret Key Generation: quantification, reconciliation and amplification schemes generating secret keys from shared radio channel estimations. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent2]
SP	Secure pairing: secured association of legitimate Nodes and terminal with Tag Signals into Interrogation and Acknowledgement Sequences, build from on-going shared radio channel estimations in the same manner of a key-free Identification Friend of Foe system. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent1]
TDD	Time Division Duplexing
TRANSEC	Transmission Security: TRANSEC is relevant to the protection of the waveform face to interception/direction finding of the transmitted radio signal, to jamming of the user receiver, and to intrusion attempts into the radio-communication access protocol. It applies mainly at the radio interface.
TS	Tag signal: Low power signal, which can be transmitted in a self-interfered scheme, at the same time (same frame or slot) and at the same carrier than the user signal (such as in Full Duplex RATs). They are used in IAS to securely pair transmitter and receiver and support accurate and authenticated channel estimations.
Tx Rx	Transmitter Receiver.

1- Declaration by the scientific representative of the project coordinator

I, as scientific representative of the coordinator of this project and in line with the obligations as stated in Article II.2.3 of the Grant Agreement declare that:

- The attached report represents an accurate description of the work carried out in this project for this reporting period;
- The project (tick as appropriate) [3]:

  ☐ has fully achieved its objectives and technical goals for the period;

  X has achieved most of its objectives and technical goals for the period with relatively minor deviations;

  ☐ has failed to achieve critical objectives and/or is not at all on schedule.

- The public website, if applicable

  X is up to date

  ☐ is not up to date

- To my best knowledge, the financial statements are in line with the actual work carried out and are consistent with the report on the resources used for the project
- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status. Any changes have been reported under section 3.2.3 (Project Management) in accordance with Article II.3.f of the Grant Agreement.

Name of scientific representative of the Coordinator: François DELAVEAU.

Date: 23/02/2017

[3] If either of these boxes below is ticked, the report should reflect these and any remedial actions taken.

2- Events following the PPR2 and the extra review PPR3 – Relevant actions and works done during the period 3.

2.1- Introduction to the document

This document is the final periodic report of the Phylaws project (numbered D1.4, referenced [PHYLAWS_D.1.4_PPR4), as specified in the updated DoW of the project [PHYLAWS_GA-DOW2]. It deals with overall results, management and cost issues of the PHYLAWS project during its 3rd period: from the 1st of July 2015 to the 30th of October 2016 (meaning M33 - M48), including updates of risk analyses and ethical issues.

This document also reflects the complete status of project activities during period 3 by including and upgrading:

- The management and cost issues of periods M33-M39, which are already covered by the intermediate technical report [PHYLAWS_D.1.3_PPR3] and the associated slides [PHYLAWS_D.1.3_PPR3slides] presented in Brussels 2016 March 30th.
- management and cost issues of periods M39-M41 and M41-M44 which are already covered by the Quarterly Month Reports QMR1 [PHYLAWS_D.1.3_qmr1] and QMR2 [PHYLAWS_D.1.3_qmr2].

There are some redundancies in this document with the previous management documents of the period mentioned above. Thus, for a better understanding of the document:

- *the text common or redundant with previous document [PHYLAWS_D.1.3_PPR3_V1.2] is written in italic,*
- the new text (relevant to period M39- M48) is written in normal font.

In addition, this document includes syntheses of complete achievements of the Phylaws project: recall of all deliverables into WPs, recall of major steps and results of WPs.

This document is completed by slides [PHYLAWS_D.1.4_PPR4slides] that supported the final review PPR4 of period 3 (held the 21st of December 2016 in Brussels – see agenda proposal and conclusion of the review in annex 1). These slides include:

- the technical part of the PPR4
- more details about the work achieved in technical Work Packages WP2 to WP6
- actions concerning dissemination (WP1 T1.2) and standardization (WP1 T1.3) led during the last period of the PHYLAWS project,
- Advisory Board issues (WP1 T1.4) and general management issues (WP1 T1.1).

Note that the released version 2.0 of this document updates the preceding version V1.0 by taking into account the remarks and recommendations of the reviewers expressed in their consolidated report [PHYLAWS_GA-CR_OL4] [PHYLAWS_GA-CR_PPR4]. It is also completed by a synthesis report (deliverable D1.5 [PHYLAWS_D1.5]) that recalls all the results and impact issues of the project.

2.2- Recall of the project context and objectives

Preliminary note for a better understanding of this section.

- *in italic font: text common with previous documents [PHYLAWS_D.1.3_PPR3] relevant to first half of period 3 (*M33- M39*) recalled here for a complete overview of period 3 activities,*
- in normal font: new text relevant to second half of period 3 (M40-M48).

The Phylaws project addresses the PHYsical LAyer Wireless Security (Physec) of public wireless networks. Phylaws intends to design new key free privacy schemes for wireless networks by exploiting the randomness of radio-propagation and to demonstrate the possibility in realistic environments:

- *to provide a radio advantage to legitimate transmitters and receivers when they face any kind of threats (eavesdropper, protocol aware jammer, spoofing systems),*
- *to generate secret keys and apply secrecy codes. The ultimate goal is to achieve optimized secrecy of network's signalling, of subscribers' private data and of communication messages.*

Phylaws' solutions intend:

- *to apply to both existing and future Radio Access Technologies (existing 2G/3G/4G/WLAN, future 5G)*
- *to apply to real radio environments (i.e. not only models of networks and radio-channel): the project includes the development of a test bed and intensive experimental tasks in real networks*
- *to take into account realistic topologies and constraints of radio networks (requested data rate for signalling and communication services, data overhead for coding, integrity control and ciphering if any, quality of service, spectrum efficiency)*
- *to deal with protocol constraints issued from standard definition (finite message lengths, flaws in signal modulation and coding)*
- *to deal with nodes' and terminals' constraints and limitations: limited embedded computing capabilities, limited power consumption.*

Figure 1 below illustrates the basic study configuration which involves a legitimate transmitter Alice, a legitimate receiver Bob and an eavesdropper Eve. Eve is not only passive but she may also have jamming and spoofing capabilities, especially to disturb or impersonate Alice and Bob at the start of the legitimate communication (negotiation phases).

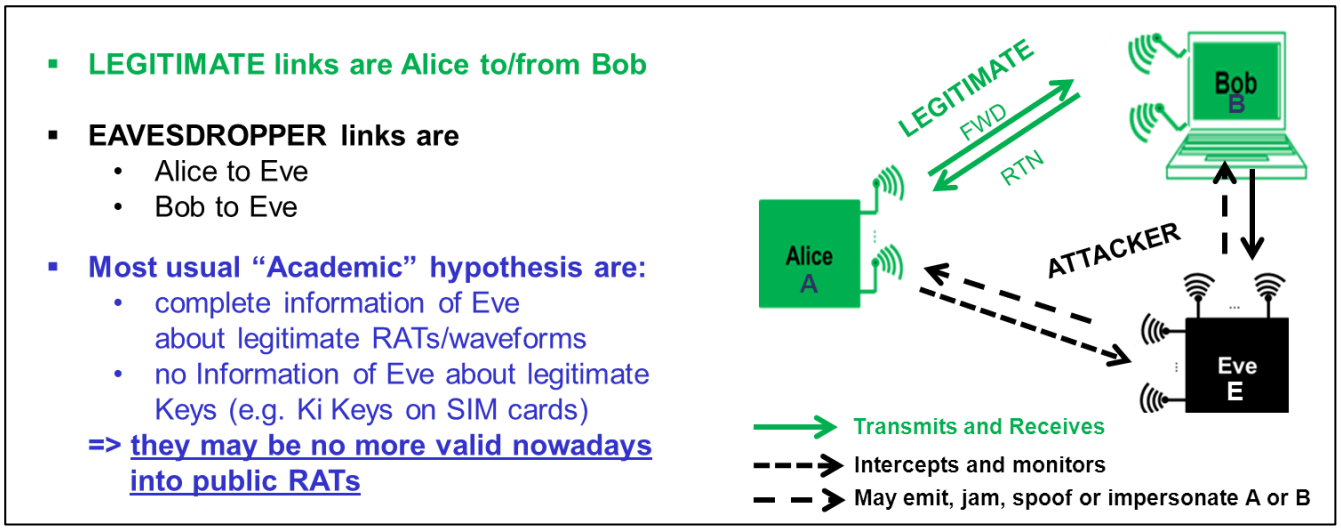


Figure 1: Problem studied by Phylaws - Illustration of the wiretap channel and several kind of threats

We recall in the Figure 2 below the organization of the Phylaws project in 6 work packages from its new DoW redaction (see [PHYLAWS_GA-DOW2]).

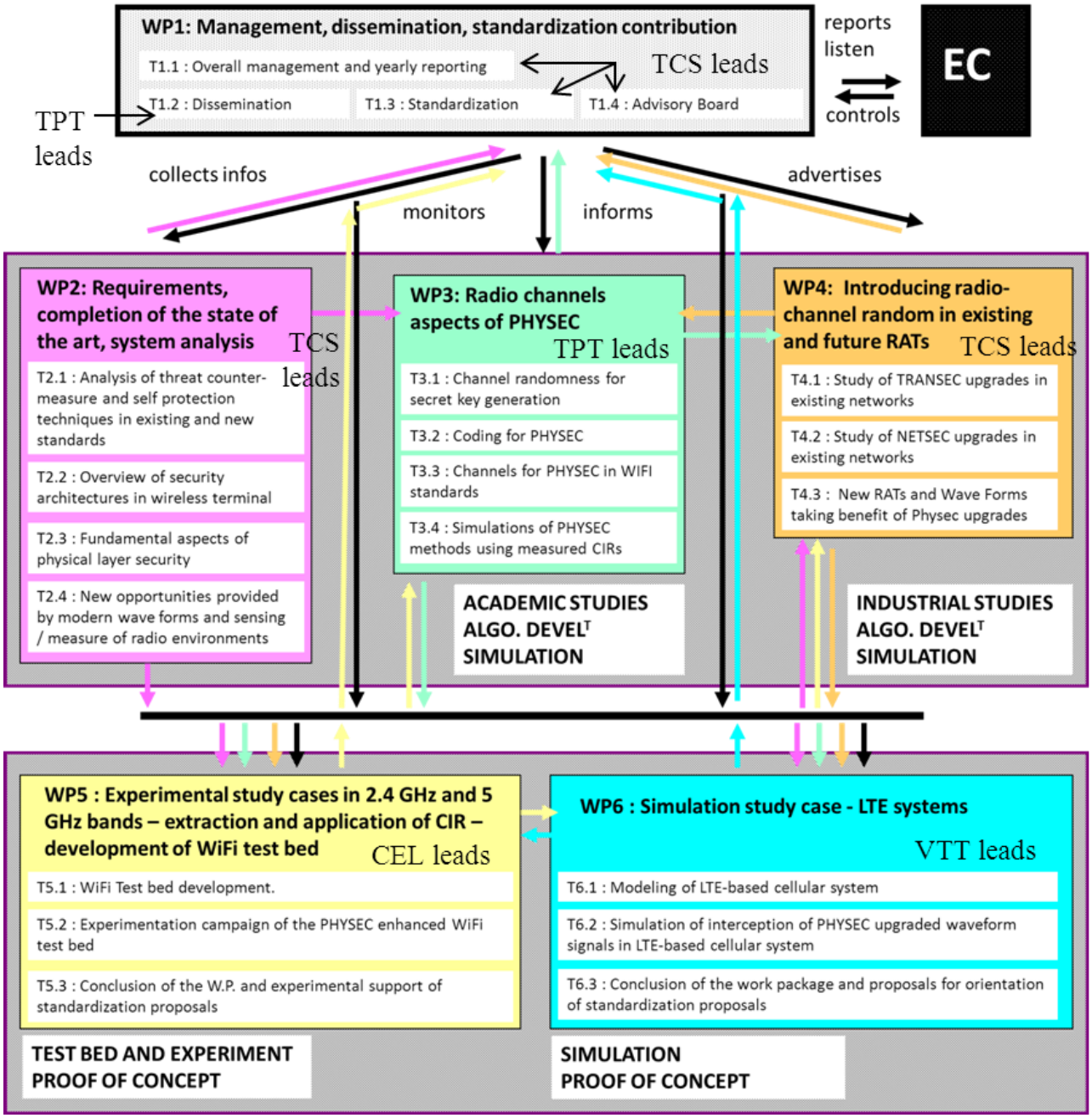


Figure 2: Recall of the Phylaws project organisation

The actualized deliverable list is given in section 2.4 (for comparison, the initial deliverable list issued from [PHYLAWS_GA-DOW2] is given in Annex 2).

The complete delivery planning of milestones and deliverables achieved during the project is given in § 3.4 (including added delays, new versions, justifications), while resource use is detailed in section 3.5 and costs expenditures are detailed in section 3.6.

We recall that a complete synthetic exposition of legitimate and attacker radio signals is given in [PHYLAWS_D.2.1] § 8.1. Short descriptions of passive eavesdropper and active attacker models (Intelligent Jammers, Man In The Middle) are also given in [PHYLAWS_D.2.1] § 8.2, while the main notions and principles relevant to physical layer security are synthetized in [PHYLAWS_D.2.1] § 8.3.

We also recall complete explanations of the project achievements during period 1 and 2 are given in section 3.2 of deliverable D1.3 [PHYLAWS_D.1.3]. Recalls use *italic font*.

2.3- Synthesis of the period 3 activities (months 33-48)

We briefly summarize the work done by the project during period 3 (M33-M48) in the eight main following items. Complementary details can be found in section 3 (description of deliverables content, IPR and patent issues, risk management issues, etc.)

Preliminary note for a better understanding of this section.

- *in italic font: text common with previous documents [PHYLAWS_D.1.3_PPR3] relevant to the first half of period 3 (*M33- M39*) recalled here for a complete overview of period 3 activities,*
- in normal font: new text relevant to second half of period 3 (M40-M48).

A/ End of academic studies (WP3):

A1/ During the first half of period 3 (M33-M39)

- *Reports D3.2 and D3.3. were delivered and published.*
- *Ms. Taghrid Mazloum prepared and successfully defended her PhD thesis at Telecom Paris Tech (Defense on February 12th, 2016).*

A2/ During the second half of period 3 (M40-M48)

- Academic and industrial partners intensified the exploitation of signals records performed during period 2 in order to prevent added delays in the firmware development of the Wifi test bed,
- This intensified exploitation of signals records also provided inputs to algorithm developments of WP4, to test bed processing and validation in WP5 and to simulation in WP6.
- The expertise of academic was involved in the analysis of algorithm development (WP4), experiment (WP5) and simulation (WP6) results.
- The Wifi test bed development was only achieved at the end of period 3. Indeed, massive recording of dual sense CSI available during the last month of the project allowed to write:
    - a significant deliverable D3.4 [PHYLAWS_D3.4] relevant to CSI measurements with the Wifi test bed,
    - a consistent deliverable D3.5 [PHYLAWS_D3.5] concluding WP3 with the exploitation of long duration channel measurement, that first enhances the feasibility proof of our Physec schemes, then re-enforces the results of the security analysis with more accurate estimations of the entropy and mutual information of the legitimate and attacker radio-channels.

B/ Continuation and end of industrial studies and development (WP4)

B1/ During the first half of period 3 (M33- M39)

- *Generation schemes of Tag Signals used in Secure Pairing were investigated and completed.*
- *SKG schemes were developed, tested and tuned with the help of real field radio channel records performed during period 2.*
- *SC schemes were developed, tested and tuned with the help of real field radio channel records performed during period 2.*
- *Deliverables D4.2 [PHYLAWS_D4.2] and D4.3 [PHYLAWS_D4.3] were delivered and published.*
- *Software codes relevant to SKG schemes and to SC schemes were developed and disseminated among partners:*
    - *developed by academics: Wallace Channel Quantization Alternate algorithm (CQA), NIST tests, nested polar codes,*

- *developed by TCS: CIR estimation, Channel decorrelation, Key reconciliation, secret amplification, Polar and Reed Muller (RM) coder and decoder, Secrecy Coding with nested polar/RM outer codes and LDPC/convolution inner codes,*
- *implanted in test bed by CELENO: Channel estimation on Wifi Non Packet Data,*
- *implanted in simulations by VTT: Tag signal generation, SKG scheme and SC scheme under LTE cellular links.*

B2/ During the second half of period 3 (M40-M48)

- Enhancements of Polar and LDPC decoding algorithms were studied by TCS (following advice of reviewers at PPR3 [PHYLAWS_GA-CR_PPR3]). New results were included into deliverable D4.4.
- Deliverable D4.4 [PHYLAWS_D4.4] was delivered and published. It completes deliverables D4.1 D4.2 and D4.3. It includes our latest results on Physec-based processing and all the technical arguments of the related feasibility proofs.
- Deliverable D4.5 [PHYLAWS_D4.5] was delivered and published. It includes the security analysis of Physec-based schemes developed during the project when facing nominal threats. D4.5 also includes several add-ons proposals to secrecy coding derived from crypto skills for enabling key-free authentication and integrity control of messages in addition to secrecy.
- Deliverable D4.6 [PHYLAWS_D4.6] was delivered and published. It includes the security analysis of Physec-based schemes when facing ultimate threats. D4.6 also concludes WP4 with a synthesis of the security analyses and a synthesis of the technical content of our proposals to standardization bodies.

C/ Continuation and end of experimental developments (WP5):

C1/ During the first half of period 3 (M33-M39), academic and industrial partners intensified the exploitation of signals records performed during the period to sustain the development of the test bed

- *First radio channels estimates were produced by the test bed in 5 GHz band (CEL) and exploited in SKG computation (TCS). Calibration problems for observing channel reciprocity were investigated.*
- *Deliverable D5.1 [PHYLAWS_D5.1] was delivered and published (final version in March 2016).*
- *Deliverable D5.1 [PHYLAWS_D5.2] was delivered in draft version March 2016, the final version being published in April 2016.*
- *D5.3. draft version was delivered and published end March 2016 (the final version being waited December 2016).*

C2/ During the second half of period 3 (M40-M48) numerous completions of the Wifi test bed development activities were done leading to experiments at 5 GHz and 2.4 GHz carriers and redaction of deliverables:

- The firmware of the test bed was strongly updated
  - to enable an efficient (even off-line) dual sense calibration of Wifi devices into the Tx and Rx chains
  - to enable explicit-beam forming prior to secrecy coding
- The test bed processing software was updated to include the completed SKG processing provided by partners TCS and TPT (Matlab versions of all algorithms: channel de-correlation pre-processing, Channel Quantization Alternate, reconciliation with error coding; privacy amplification with hash functions, etc.)
- The test bed processing software was updated to package the completed SC processing provided by partners TCS and ICL (Matlab versions of all algorithms: polar coding/decoding, Reed Muller coding/decoding, etc.)

- Massive experimentations of the Wifi test bed occurred during summer 2016 which produced calibrated dual sense CSI for SKG processing and AN-BF configurations for SC processing over a few snapshots first, then over long time durations.

  Note that the relevant results were presented during the Phylaws workshop at PIMRC'2016 Valencia and significantly sustained the last standardization initiatives of the Phylaws consortium at 3GPP and ITU.

- Intensive redaction of late deliverables occurred during autumn 2016:
  - final version of D5.3 [PHYLAWS_D5.3]
  - D5.4 [PHYLAWS_D5.4] including complete reporting of experiments with the test bed,
  - D5.5 [PHYLAWS_D5.5] concluding the WP5 with recommendations for standardization,

  all these deliverables were published in December 2016.

D/ Continuation and end of simulation developments (WP6):

D1/ During the first half of period 3 (M33-M39),

- *An upgraded version of D6.1 [PHYLAWS_D6.1] was delivered and published in March 2016: answering to reviewer remarks expressed during the PPR2 [PHYLAWS_GA-CR_PPR2].*
- *Redaction of D6.2 [PHYLAWS_D6.2] was initiated.*

D2/ During the second half of period 3 (M40-M48)

- The simulator processing software was updated to package the completed SKG processing delivered by partners TCS and TPT (as for WP5 above: Matlab versions of all algorithms)
- The simulator processing software was updated to package the completed SC processing delivered by partners TCS and ICL (as for WP5 above: Matlab versions of all algorithms)
- Deliverable D6.2 [PHYLAWS_D6.2] including the simulation plan and first simulation results was completed, submitted and published in May 2016.
- Massive simulations occurred during the spring and the beginning of summer 2016 which produced accurate evaluations of Secure Pairing (TS and IAS), SKG and AN-BF+SC schemes under LTE carriers over a significant variety of geometry and radio propagation environments.

  Note that the relevant results were presented during the Phylaws workshop at PIMRC'2016 Valencia and significantly sustained the last standardization initiatives of the Phylaws consortium at 3GPP and ITU.

- Deliverable D6.3 [PHYLAWS_D6.3] was published September 2016. It concludes WP6 with complete simulation results and recommendations for standardization.

E/ Continuation and conclusion of dissemination activities (WP1 T1.2, D1.8):

E1/ During the first half of period 3 (M33-M39),

- ***The web site was continuously updated*** *with*
  - *Papers and presentation published by the consortium;*
  - *PhD Thesis of Dr.Taghrid Mazloum (Dissertation report and presentation slides) and Hamed Mirghasemi (Dissertation report) are uploaded at the public web site www.phylaws-ict.org);*
  - *updated versions of deliverables D2.1, D2.4, D4.1;*
- *All our new deliverables were published: D3.2, D3.3, D3.4 preliminary partial version, D4.2, D4.3, D5.1, D5.2, D6.1, D5.3 draft version.*

- *New presentations at Winncomm forum Europe 2015 and Two new papers and presentations at Winncomm forum USA 2016.*
- *One paper and one presentation at the ETSI Workshop on Air Interface Sophia Antipolis January 2016*
- *One journal publication paper "Analysis of Secret Key Randomness Exploiting the Radio Channel Variability" in the International journal of Antennas & propagation (IJAP), Sept. 2015*
- *One presentation at the MILCOM 2015 panel on secure communications for civilian applications of unmanned aerial systems, October 2015*
- *Submission of a Workshop proposal at PIMRC 2016 (Valence Spain 4 - 7 September 2016), which was accepted in March 2016.*

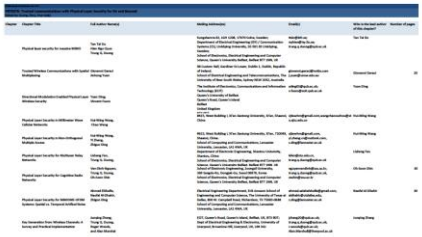
E2/ During the second half of period 3 (M40-M48)

- **Preparation of the WS dedicated to Physec at PIMRC 2016** (Valence Spain Sunday 4 September 2016 morning), after acceptance in March 2016 in a reduced version (one half day instead of a full day as initially proposed).
- **Preparation of new publications,** including especially:

  Two journal papers for the Springer Journal Special Issue on Analog Integrated Circuits & Signal Processing (publication early 2017). This follows the publication of our two papers at the Winncomm Forum US, Reston 2016, and their selection (end April 2016) by the Wincomm Forum committee for journal publication. Note that these journal papers will include the dual sense SKG results input by the CSI measured with the test bed and some of our most advanced results on Secrecy Coding, establishing the feasibility proof and the reliability of these two security schemes and providing arguments for further optimized implementations.

- **Organization of the project final WS at PIMRC'2016**, which was held on Sunday 4th of September at the Valencia Congress center. Then publication the relevant papers an presentation at the Phylaws Web site (see http://www.phylaws-ict.org/?page_id=21)

- Two book chapters into a book dedicated to Physical layer security (publication planned 2017). This book is entitled "Trusted Communications with Physical Layer Security for 5G and Beyond". It is edited by Trung Q. Duong, Xiangyun (Sean) Zhou, and H. Vincent Poor and published by IET Publisher. The Phylaws consortium is in charge of writing chapter 19 ("Application cases of Secret Key Generation in communication nodes and terminals") and 20 ("Application cases of Secrecy Coding in communication nodes and terminals"). Each chapter was first submitted in November 2016. The publication will occur year 2017. They are about 30 pages each. The list of the book content and of its authors is given in the attached file below.



- **Continuous updates of the web site** with dissemination actions papers presentations etc.
- **Redaction of deliverable D1.8 [PHYLAWS_D1.8] which concludes WP1 Task T1.2** with a complete reporting of dissemination actions of the period 3 of the PHYLAWS project (while D1.7 [PHYLAWS_D1.7] deals with dissemination over period 2 and D1.6 [PHYLAWS_D1.6] deals with dissemination plan and dissemination actions over period 1).

F/ Continuation and conclusion of standardization activities (WP1 T1.3 D1.11)

F1/ During the first half of period 3 (M33-M39),

- ***Contributions to EDA:***
  - *Following the contacts initiated during summer 2015 with Mr. Michael Sieber, who is the head of the unit "Information Superiority" at the European Defense Agency [EDA_WP], Phylaws was invited to present its security concepts and intermediate results at the EDA "Capability-Technology Groups (CapTechs)" during the joint session of the 31st CapTechs meeting which was held on the 10th of November 2016 in Brussels.*
  - *The consortium was invited to present a synthesis of the results achieved in PHYLAWS after the end of the project (e.g. during year 2017).*
- ***Contributions to ETSI:***
  - *Following the paper and the presentation at the ETSI Workshop on Future Radio Technologies: Air Interface (Sophia Antipolis, France, January 2016), Thales participates in Working Group relevant to "modulation tool boxes" including physical layer security aspects.*
- ***Participation to 3GPP SA3#80 in Tallinn, Estonia (August 2015):***
  - *Discovering of the current areas of interest of SA3 in order to identify the best opportunities for the implementation of Physec*
  - *Presentation of contribution S3-152075 by Thales and VTT, centered on application cases of SKG and based for the protection of the first signaling messages, sustained by the results of deliverable D4.3 [PHYLAWS_D4.3] plus simulations and analysis led in WP6.*

- ***Participation to 3GPP SA3#82 in Dubrovnik, Croatia (February 2016):***
  - *Presentation of a discussion paper on the physical layer security focusing on secret key generation and secrecy coding. The reference of the document is S3-160267 (cf. D1.11)*
  - *Participation to the elaboration of a new Study Item "Study on Architecture and Security for Next Generation System" dealing with the security architecture of 5G systems. The content of the future study item is described inside document S3-160278 (cf. D1.11). During the discussions, Thales insisted on the following points:*
    - *To include investigations about "secure access"*
    - *To give the possibility to "include standalone security topics" within the framework of this study item. Thus, SA3 will not be limited to SA1 and SA2 requirements but will be able to innovate and to propose new security solutions.*
  - *The new study item on 5G was approved by SA plenary meeting held in Gothenburg, Sweden in March 2016.*
- ***Participation to the 23rd meeting of the ITU-R Working Party 5D in Beijing, China from February 23 to March 2, 2016.***
  - *Submission of two contributions under the French administration authority.*
  - *The first contribution resulted in the addition of radio access security aspects in the draft of the Report ITU-R M.[IMT-2020.SUBMISSION] "Requirements, evaluation criteria and submission templates for the development of IMT-2020". Radio Interface Technologies candidates to the IMT2020 label had to describe how they address the radio access security. Thales intended to contribute to this report for items relevant to security of radio access and to Physical Layer Security. Nevertheless, diplomatic work had still to be achieved in order to assess items relevant to physical layer security.*
  - *The second contribution yield to the possible opening of a new study report on Machine-type communications with a section dealing with security aspects including considerations on "secure radio access". More contributions on this topic occurred during the next ITR-R WP 5D meeting (June 2016). The structure of the report had to be defined, same for the chairman of the drafting group.*

F2/ During the second half of period 3 (M40-M48)

- **Pursuit of presence at ETSI:**
  - Phylaws submitted a special paper and gave a presentation at "ETSI Workshop on Future Radio Technologies: Air Interfaces" held on 27th – 28th of January in Sophia Antipolis, which combined results and redactions of project Prophylaxe and Phylaws.
  - At the special workshop entitled "International Workshop RVM and security for multi-RAT reconfigurable system", organized by B-COM/ETSI in Cesson Sevigné (France) in March 2016 with a presentation updating the combined results of project Prophylaxe and showing first dual sense SKG results input by the CSI measured with the test bed at wifi carrier 5 GHz.
  - At the ETSI security week in Sophia Antipolis (June 2016).
  - At the 5G Ensure security Work Shop in Sophia Antipolis (June 2016).
- **Pursuit and conclusion of contributions at 3GPP:**
  - *Participation and contributions to 3GPP SA3#82 in Dubrovnik, Croatia February 2016: see above*
  - **Participation and contributions to 3GPP SA3#83 meeting held in San Jose del Cabo (Mexico), 9-13 May 2016,** with the following objectives

- To create a security area dedicated to the protection of the signaling over the Uu interface, i.e between the base station (or eNB in 4G) and the mobile (or UE).
- To propose a key issue entitled "Reducing interception capability over the Uu interface" to highlight the current vulnerability of the Uu interface against attack. This flaw enables an eavesdropper to retrieve crucial information that can jeopardize the establishment of confidentiality, integrity and privacy.
- To propose Physec-based technologies, such as SKG, beamforming and SC schemes as potential solutions for this key issue through original contributions S3-160641 "Protection of signaling over the Uu interface" then revised into contribution S3-160785 in order to fit with the new security area "RAN signaling
- To support other discussions and proposals relevant to security items such as:
  - S3-160551 "pCR to TR 33.899 High Level Security Requirement on Authentication"
  - S3-160552 "pCR to TR 33.899 User awareness and control"
  - S3-160437 "pCR to TR 33.899: Security resilience issues and solutions"

- **Participation and contributions to 3GPP SA3#84 meeting held in Chennai (India), 25th – 29th July 2016,** with the following objectives:

  - To submit the discussion paper S3-161019 (mainly based on the analysis led in Deliverable D2.1 [PHYALWS_D2.1]) that clearly exposes the threats of current 3GPP system, especially concerning the radio air interface vulnerabilities.
  - To introduce contribution S3-161017 which aimed at being inserted into Technical Report 33.899 entitled "Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system" (release 14)". According to advice from SA3, Thales adapted its strategy by proposing only a "key issue" without any direct relationship to Physec-based solution, keeping the key issue open enough to avoid censure of stakeholders. Note that contribution S3-161017 proposed to study how to exchange sensitive data before the establishment of a security context.

    Note that this proposal was criticized by stakeholders. Beyond these critics, there were mainly rivalries between competing solutions.
  - To present contribution S3-161011 "pCR for adding security assumptions on 5.4 security area #4: RAN security" which aimed at defining the security framework of the security area RAN security. This contribution suffered from same kind of critics from stakeholders that want as most as possible prevent the introduction of potential security requirements favorable to physical layer security concepts.
  - To support other security topics that could take advantage of the physical layer protections, such as:
    - The enhancement of the subscriber privacy. Thales supported the definition of Key issue #7.2: Concealing permanent or long-term subscriber identifier, Key issue #7.3: Concealing permanent or long-term device identifier, Key issue #7.4: Using effective temporary or short-term subscriber identifiers Key issue #7.5: Transmitting permanent identifiers in secure interface, Key issue #7.7 Using effective temporary or short-term device identifiers.
    - Security Implications of Low Latency: The relavant key issue #1.13 highlights the security problems related to low latency communications while the current security protections appear to be too slow to meet the new requirements specified by SA1. Therefore, Physec could provide faster protection mechanisms.

- **Participation and contributions to 3GPP SA3#84b meeting held in San Diego (27th – 29th September 2016),** with the following preparation and objectives:

  - To build contributions upon approved key issues and security requirements. Our strategy was to shift from a debate on the reality of the threats (cf. meeting SA3#83 and SA3#84), to a debate on the proposed solutions. Moreover, TCS decided not to contribute anymore in the security area #4 RAN security that appeared to be a topic not willing to innovation, and to focus on more open-minded security areas.

  - To submit contribution S3-161414 "pCR for adding a solution for key issue #1.13: Security Implications of Low Latency", to solve the security issue with low latency requirements with AN-BF and SC (as identified during SA3#84).

  - To Submit contribution S3-161404 « pCR for adding solution for key issues #7.4 and #7.7: effective generation of temporary or short-term identifiers based on channel estimation" that proposes to use the randomness of the channel estimation and parts of SKG processing to generate a key used as a temporary identifier. Due to the lack of time, the presentation of this contribution was postponed to SA3#85.

  - To submit contribution S3-161405 "pCR for adding solutions for key issues #7.2: Concealing permanent or long-term subscriber identifier with opportunistic encryption", that proposes an opportunistic encryption of IMSI exchanged between the User Equipment (UE) and the base station by either SKG or Diffie-Hellman processing; SKG requiring less computing capabilities than DH in TDD case. Due to the lack of time, the presentation of this contribution was postponed to SA3#85.

  - To present the discussion paper contribution S3-161427 "Discussion on key-free secured pairing and protected radio access to network" relevant to the secure pairing protocol based on tag signals and IAS designed in WP4 (see deliverable D4.1 [PHYLAWS_D4.1], D4.2 [PHYLAWS_D4.2] and D4.5 [PHYLAWS_D4.5]). Due to the lack of time, the presentation of this paper was postponed to SA3#85

- **Participation and contributions to 3GPP SA3#85 meeting held in Tenerife (7th – 11th November 2016),** with the following preparation and achievements:

  - To obtain the approval for contribution S3-161404 « pCR for adding solution for key issues #7.4 and #7.7: effective generation of temporary or short-term identifiers based on channel estimation". After approbation by SA3, the contribution was revised in document S3-162101 with requirements for more details to be written in the document for the next meetings (SA#86 Sofia Antipolis February 2017)

  - To obtain the approval for contribution S3-161405 "pCR for adding solutions for key issues #7.2: Concealing permanent or long-term subscriber identifier with opportunistic encryption", which final approved version S3-161620 captures the concern of active attacks. Note that this document mentions for the first time in 3GPP SA3 the possibility to use Secret Key Generation in a protection mechanism.

  - To submit, in collaboration with Interdigital, a proposal to add a new key issue for the protection of the entire IMSI. The document was approved after some modifications requested by other companies that led to the revised contribution S3-161200. Note that the approval of this key issue was a crucial point to obtain the final approval of contribution S3-161620

  - Contribution S3-161427 "Discussion on key-free secured pairing and protected radio access to network" was one more time postponed due to the lack of time and should be discussed in next SA3#86 meeting in Sophia Antipolis next February 2017.

  Important Note: The next SA3 meeting will be SA3#86 to be held in Sophia Antipolis (France) between the 6th and the 10th February 2017 and the TCS will be present to achieve the final concretization of his standardization initiatives.

Important Note about standardization networking: mutual support of standardization proposals was set at 3GPP meetings with the 5G Ensure team and persons of Thales who represents TCS at several groups of 3GPP (SA3, SA6, RAN).

- **Pursuit of and conclusions of contributions at ITU WP 5D:**
  - ***Participation and contribution to the 23rd meeting of the ITU-R Working Party 5D in Beijing, China February 23 - March 2, 2016:*** *see above*
  - ***Participation and contribution to the 24th Meeting of the ITU-R WP 5D (14 – 22 June 2016, Geneva, Switzerland):***
    - With the collaboration French administration and with the support of the German administration, the Phylaws team prepared a contribution on the opening of a new report on MTC entitled Proposal for a *"New Report on Technical and Operational Aspects of Machine-Type Communications"* which was submitted by TCS on behalf of THALES SA.
    - A working document was created (from a proposal of Telefon AB – LM Ericsson) towards a preliminary draft new report on the usage of International Mobile Telecommunication (IMT) for verticals referenced M.[IMT2020.SUBMISSION]. Material from other contributions was added within the working document. Specifically, the section on security of the Thales contribution above was included within the IMT capabilities of the draft report. Security aspects considered by TCS were authentication, privacy, integrity and confidentiality.
  - **Participation and contribution to the 25th Meeting of the ITU-R WP 5D (4 – 12 October 2016, Geneva, Switzerland),** with the following objectives preparation and contributions:
    - The objective of Phylaws team for this meeting was twofold: First, to convince all administrations and companies to integrate security aspects among capabilities of IMT systems in the draft new report mentioned above; second, verify that the contributions of Phylaws team within the security section of the draft new report would not be altered during the meeting.
    - Following the discussions of the previous meeting, the Phylaws team prepared in collaboration with the French administration a contribution on security aspects of IMT systems entitled "Considerations on Security Aspects of IMT Networks for the Working Document towards a Preliminary Draft New Report referenced M.[IMT-BY OTHER INDUSTRIES]", which was submitted on behalf of THALES SA. This contribution was presented by TCS team within the ITU Usage: TCS had to first convince on the importance of security for Machine-Type Communication, particularly for critical use cases such as Ultra-reliable and low latency communications (urLLC) and then to negotiate with other delegations (US delegation mainly) the inclusion of major part of the contribution into the future report.
    - Concerning the draft new report the M.[IMT2020.SUBMISSION] TCS verified that no changes were made in the security section.

- **Redaction of deliverable D1.11 [PHYLAWS_D1.11] which concludes WP1 Task T1.3**

  D1.11 includes a complete reporting of standardization actions of the period 3 of the PHYLAWS project while
  - D1.10 [PHYLAWS_D1.10] deals with standardization initiatives planned during period 2
  - D1.9 [PHYLAWS_D1.9] presents our initial standardization plan).

G/ Continuation and end of Advisory Board activities (WP1 T1.4, D1.14):

During the first half of period 3 (M33-M39),

- *The second advisory board meeting was organized on 20 January 2016, and hosted in Telecom Paris Tech (partner TPT).*
- *Deliverable D1.13 [PHYLAWS_D1.13] has been delivered and published in February 2016.*

During the second half of period 3 (M40-M48)

- **The third Advisory Board meeting was cancelled**: while the initial idea of the Phylaws consortium was to organize the AB meeting through a round table organized at workshop WS8 dedicated to Physical Layer Security hosted in PIMRC 2016 Valence Spain, Sunday 4th of September 2016 (see section 2.3 – E above), the PIMRC'2016 technical committee decided to limit the Workshop to one half day. It was no more possible to hold our initial proposed planning over a full day concluded with a panel inviting our Advisory Board, and the TCS's choice was to focus his last effort on his latest standardization initiatives, while serious concretization perspectives appeared during the summer 2016 (see section 2.3 – F above).

- **Deliverable D1.14 [PHYLAWS_D1.14] has been delivered and published**: it includes a synthesis of the advisory board activities advice over the duration of the Phylaws project. In addition, it syntheses how the Phylaws team applied this advice at technical development, at dissemination strategy and at standardization strategy.

H/ Other Management activities:

H1/ Deliverable submission and publication (See § 2.4 for a synthesis, § 3.3.4 for more details)

During the first half of period 3 (M33-M39):

N*ew deliverables D3.2, D3.3, D3.4 preliminary partial version, D4.2, D4.3, D5.1, D5.2, D6.1, D5.3 Draft versions were submitted and published*

During the second half of period 3 (M40-M48):

New deliverables D3.4 final completed version, D3.5, D4.4, D4.5,D4.6, D5.3 final version, D5.4 D5.5, D6.2, D6.3, D1.8, D1.11 and D1.14 were submitted and published

H2/ Discussion and collaboration with other funded projects (See § 3.3.6 for more details):

During the first half of period 3 (M33-M39),

Contacts occurred with the FP7 project Duplo. They led to concrete estimations of order of magnitude of Self Interference Mitigation performance into Full Duplex RATs, which is a key input parameter for the building of the Tag Signals and the tuning of the Tag to Signals ratio (intentional self-interference of TS) into the Secure Paring scheme we proposed and patented.

Since a first meeting during the ICC London in June 2015 and the organization of a common workshop in August 2015, the Phylaws teams worked with the Prophylaxe project in the following directions:

- *Confirmation of SKG capabilities and performance for Machine-type communications and IoT, feasibility proof of SKG input with channel information limited to CSI magnitude* (which was proven again in our Wifi records in NLOS case (see D3.5).
- *Order of range of radio-channel diversity in very fixed geometry and relevant latencies for radio-channel de-correlation and SKG.*
- *Joint dissemination and standardization effort and especially*
  - *common publications at ETSI (see section 2.3- E above)*

- *preparation of common standardization initiatives at 3/5 GPP (see section 2.3 - F above)*
- *preparation of common standardization initiatives at ITU (involving national French and German administrations, see section 2.3 - F above)*
- *Mutual inputs for paper redaction (ex: EUCNC 2016).*

The Phylaws teams took the initiative of contact other funded projects such as 5G-Ensure and asked for participation in their initiatives.

During the second half of period 3 (M40-M48)

- A meeting held end March (2016-03-22) for Thales teams of projects Phylaws, 5G-Ensure, Coherent, and Sonata, was organized by TCS commercial people (Mrs Sylvie Raynaud) where the Thales teams of the following European projects were invited:
  - Phylaws (Number 317562) - TCS participant: F Delaveau, C Kameni, R Molière
  - 5G-Ensure (Number 671562) - TCS participant: Pascal Bisson
  - Sonata (Number 671517) - TCS participant: Mathieu Bouet
  - Coherent (Number 671639) - TCS participant: Antonio Cipriano

- Coordinated actions at 3GPP standardization groups occurred with the Phylaws and 5G Ensure team members and with people of TCS in charge of Thales representation at 3GPP groups (SA3, SA6, RAN).

- Coordinated actions occurred at ITU-R working groups
  - with the direct collaboration of the French administration
  - with the active support of foreign administration such as German, Finland
  - with the agreement of other foreign administration such as USA, after negotiation

In addition, the Phylaw team participated to the 5G Ensure security Workshop in Sophia Antipolis (June 2016).

H3/ IPR strategy (See § 3.3.7 for more details)

During the first half of period 3 (M33-M39) the IPR strategy has been defined. Three patents addressing Secure Pairing, Secret Key Generation and Secrecy Coding were written (in French) and submitted:

- *to the French DGA for publication authorization,*
- *to the French patent office (INPI) for acceptation.*

During the second half of period 3 (M40-M48), the defense of the three patents was done with the French patent office.

The next steps (after the end of the Phylaws project) are:
- Translation and extension to Europe,
- Extensions to North America, and other world regions.

See § 3.3.7 for more details.

2.4- Actualized check of the deliverables list.

The tables below recall, work package per work package and task per task, the updated list of deliverables relevant to the revised DoW [PHYLAWS_GA-DOW2] and the relevant date of delivery.

Signification of highlights

- When non-highlighted, the references are relevant to contracts and deliverables of period 1: Months 1 to 12.
- The yellow-highlighted references are relevant to contract's modifications and added deliverables that were achieved during to period 2: Months 13 to 32.
- The blue-highlighted references are relevant to deliverables of period 1 that were achieved during period 2: Months 13 to 32.
- The green-highlighted references are relevant to deliverables of period 2: Months 13 to 32.
- The grey-highlighted references are relevant to deliverables of period 1 and 2 that were upgraded during period 3 after PPR2 (hold in Brussels 9 September 2015) in order to match the recommendations of the reviewers and of the EC.
- The pink-highlighted references are relevant to deliverables of period 3 published during the period Months 33 to 40.
- The pigeon blue references are relevant to deliverables of period 3 that were published since the intermediate technical review at month 41.
- The pigeon blue underlined references are relevant to deliverables of period 3 that were published after PPR4 (after Month 50).

WP1 "Management, Dissemination, Standardization, Advisory Board"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. Level	Del. date	PM ind. (Tot= 296)	Resp
D 1.1	Kick-Off meeting. Management Plan, including risk evaluation, analysis of Ethical Issues. Minutes of K.O. Consortium Agreement.	1.1	R	PU	1	6	TCS
D 1.2	Months 1-12 (year 1) review meeting RM1 and PPR1	1.1	R	PU	12	2	TCS
D 1.3	Months 13-32 review meeting RM2 and PPR2	1.1	R	PU	32	1,5	TCS
D 1.3 PPR3	Extra technical review meeting RM3 : initial report	1.1	R	PU	40	0,5	TCS
D 1.3 PPR3 +slides	Extra technical review meeting RM3 : initial 15/3/2016, revised extra report version V 2.0 3/5/2016 version V2.1 20/5/2016 Presentation slides of the RM3	1.1	R	PU	40 43	0,5	TCS
D 1.3 qmr1	Quarterly months management report 1 for year 3 version V1.1 - date 2016-03-15 version V2.0 - date 2016-05-20	1.1	R	PU	42	0,5	TCS
D 1.3 Qmr2	Quarterly months management report 2 for year 3	1.1	R	PU	42	0,5	TCS
D 1.4	Months 33-48 review meeting RM4 and PPR4 – Synthesis – Open workshop on projects results	1.1	R	PU	>48	3	TCS
D 1.5	Synthesis of the project managT. Final release of risk analysis. Final report on Ethical Issues	1.1	R	PU	planned > 50	2	TCS
D 1.6	Dissemination planning report	1.2	R	PU	3	1	TPT
D 1.7	Dissemination intermediate report	1.2	R	PU	30	2	TPT
D 1.8	Dissemination final report	1.2	R	PU	48	3	TPT
D 1.9	Standardization planning report	1.3	R	PU	3	1	TCS
D 1.10	Standardization interm. Report	1.3	R	PU	30	2	TCS
D 1.11	Standardization final report	1.3	R	PU	48	3	TCS
D 1.12	Advisory board meeting report 1	1.4	R	PU	12	1	TCS
D 1.13	Advisory board meeting report 2	1.4	R	PU	40	1	TCS
D 1.14	Advisory board meeting report 3 - synthesis	1.4	R	PU	48	1	TCS

Figure 3: New deliverable list of the reorganized PHYLAWS project – WP1

WP2: "Requirements, completion of the state of the art, system analysis"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. Level	Del. date	PM ind.	Resp
D 2.1	Analysis of the threat counter-measure and protection techniques in existing and new standards – report	2.1	R	PU	8	6	VTT
D 2.2	Security architectures in wireless terminal – report	2.2	R	PU	10	6	TCS
D 2.3	Fundamental aspects of physical layer security – report	2.3	R	PU	12	24	TPT
D 2.4	New opportunities provided by modern wave forms and sensing/measure of radio environments – report	2.4	R	PU	20	8	TCS

Figure 4: New deliverable list of the reorganized PHYLAWS project – WP2

WP3: "Radio channels aspects of PHYSEC"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level	Del. date	PM ind.	Resp
D 3.1	Channel based random generators – interm. report	3.1	R	PU	15	15	ICL
D 3.2	Channel based random generators – final report	3.1	R	PU	36	9	TPT
D 3.3	Coding techniques and algorithms for secrecy coding and secret key generation	3.2	R	PU	36	24	ICL
D 3.4 draft	CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band – draft version	3.3	R	CO	40	16	CEL
D 3.4 final	CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band	3.3	R	CO	48	16	CEL
D 3.5	Simulations report of PHYSEC methods using measured CIRs	3.4	R	CO	48	13	TCS

Figure 5: New deliverable list of the reorganized PHYLAWS project – WP3

WP4: "Introducing radio-channel randomness in existing and future RATs"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level	Del. date	PM ind.	Resp
D 4.1	TRANSEC upgrades of existing RATs - study report	4.1	R	PU	30	6	TCS
D 4.2	TRANSEC upgrades of existing RATs - simulation and analyses complements	4.1	R	PU	36	6	TCS
D 4.3	NETSEC upgrades of existing RATs - study report	4.2	R	PU	36	6	TCS
D 4.4	NETSEC upgrades of existing RATs - simulation analyses complements	4.2	R	PU	46	6	TCS
D 4.5	New Rats and waveforms taking benefit of Physec upgrades – interim report	4.3	R	PP	48	9	TCS
D 4.6	New Rats and waveforms taking benefit of Physec upgrades – final report	4.3	R	PP	48	10	TCS

Figure 6: New deliverable list of the reorganized PHYLAWS project – WP4

WP5: "Experimental study cases in 2.4 GHz and 5 GHz bands – extraction and application of CIR - development of the WiFi test bed"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level	Del. date	PM ind.	Resp.
D 5.1	WiFi test bed setup development report	5.1	R	PP	40	20	CEL
D 5.2	Experiment campaign plan	5.2	R	PP	40	10	CEL
D 5.3 draft	Intermediate Report on WiFi interceptor experiments with the test bed	5.3	R	PU	40	12	CEL
D 5.3 final	Intermediate Report on WiFi interceptor experiments with the test bed	5.3	R	PU	>48	12	CEL
D 5.4	Final report on interception experiments on test bed, synthesized with complementary simulation results. Final analyses on PHYSEC methods proof of concept	5.4	R	PU	>48	10	CEL
D 5.5	Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades	5.5	R	PU	>48	12	CEL

Figure 7: New deliverable list of the reorganized PHYLAWS project – WP5

WP6: "Simulation study case – LTE based cellular systems"

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level	Del. date	PM ind.	Resp.
D 6.1	Modeling of LTE-based cellular system Version 1.0 June 2015 - version 2.0 February 2016	6.1	R	PU	32 40	18	VTT
D 6.2	Simulation of interception of waveform signals in LTE-based cellular system	6.2	R	PU	42	12	VTT
D 6.3	LTE-based cellular system simulations – Concluding of the work package and proposals for standardization	6.3	R	PU	47	8	VTT

Figure 8: New deliverable list of the reorganized PHYLAWS project – WP6

2.5- Following of the Second Periodic Review (PPR2, RM2) and the third intermediate technical review (PPR3, RM3) – taking into account reviewers' remarks and advice.

Following the PPR2 review of the second period (held on 2015-09-09) and the intermediate PPR3 review of the first half of the period 3 (held 2016-03-30), the table below recalls how the Phylaws project took into account the recommendations of the reviewers all over the third period of the project, included into reports of the PPR2 [PHYLAWS_GA-CR_PPR2] and [PHYLAWS_GA-CR_PPR3].

- *The first part of the table (in italic character) deals with the recommendations of the reviewers during and after PPR2 [PHYLAWS_GA-OL_PPR2] [PHYLAWS_GA-CR_PPR2]. It is relevant to the first half of period 3 (M33- M39) and details the way the project organization and realization follow them. It reproduces most of the content of the extra periodic report [PHYLAWS_D.1.3_PPR3] §2.5. The relevant repetition is assumed in the present deliverable to achieve better readability and clarification of the project coordination all over its period 3.*

- The second part of the table (in normal characters) deals with the recommendations and requirements of the reviewers during and after PPR3 [PHYLAWS_GA-OL_PPR3] [PHYLAWS_GA-CR_PPR3]. It is relevant to second half of period 3 (M40-M48), it details some remarks/answers of the coordinator describes the way followed by the project coordination and realization to match these recommendations. Here, there is no redundancy with [PHYLAWS_D.1.3_PPR3], but some parts of these answers remarks and descriptions were already included in the Quarterly Month Reports [PHYLAWS_D.1.3_qmr1] and [PHYLAWS_D.1.3_qmr2]. Also here, the relevant redundancy is assumed in the present deliverable to achieve better readability and clarification of the project coordination all over its period 3.

	Recommendations and Requirements **See details in [PHYLAWS_GA-CR_PPR2]**	**How does the project organization answer to remarks / requirements of expert reviewers and of EC. See details in the following and in the intermediate technical report [PHYLAWS_D.1.3a]**
	Ref: [PHYLAWS_GA-CR_PPR2] §a. Page 3-5	***Phylaws' answers***
A.1	*General - Quality of the results* *… lack of precision in the description of the work with statements such as 'six antennas close to each other', type of antennas used in the measurements, the number of measured locations, the choice of the measurement bandwidth in the VNA measurements etc…* *… whether the measurements were analysed in a similar manner to verify the application of such a model…* *… led the reviewers to believe that currently, the different teams are working independently with a rather limited degree of interaction…*	*All this details are completed in the Thesis of Ms. T Mazloum. Complements are in D3.4 and D3.5 which are dedicated to radio-channel measurement campaign, and deliverables of WP5 which is dedicated to test bed experiments* *Complements will be in D5.2 and D6.2.* *Such as apparent "fragmentation problems" raised by reviewers in the following of [PHYLAWS_GA-CR_PPR2] , this apparent "independent working" occurred during period 2 as a consequences of items described at line C.7.1 of this table: consequences of first periodic review, late acceptance of new DoW by EC, completion time of the experimental test bed and simulation. Right now, the project have restarted, simulation and test bed are in progress, academics and industrial partners have exchanged source codes, propagation channels etc.*
A.2	*General - Take-up of the recommendations from the previous review* *In response to the first technical review meeting (Jan. 2014), a modified, and refocused, DoW which took into account some of the reviewers' recommendations and suggestions was proposed and accepted (Oct. 2014).*	*The acceptance was 10 March 2015[PHYLAWS_GA-AM1] and not October 2014.* *This reason among others explain most of the apparent "independent working" and "fragmentation problems" of period 2 raised in [PHYLAWS_GA-CR_PPR2].*
A.3	*However, as previously stated the recommendation regarding enhanced interaction between "the activities of WP's 5 and 6 and relating them to WP's 3 and 4", was not taken up fully, and in some cases there appears to be duplication of effort.*	*See answers at line A.1 and C.7.1 of this table.*
A.4	*Contact has been made with other EU projects such as Prophylaxe and DUPLO but as yet no concrete activity is referred to in the report.* *…* *There is also lack of interaction with the set-up and subsequent running of the 5G PPP initiative … two of the project partners are members of the NetWorld 2020 ETP (one also being a member of the 5G INFRASTRUCTURE Association), and both participate in the H2020 / 5G PPP project 5G-ENSURE, which specifically addresses security issues in 5G.*	*During the start of period 3, contact with Prophylaxe led to significant outputs:* - *a common workshop (August 2015)* - *common paper and presentation at the ETSI WS on Air interface (January 2016) see more details in § 3.3.2.* - *combined effort at 5GPPP and ITU-R (February 2016) see more details in § 3.3.3.* *Phylaws initiated the contact with 5G-Ensure: see more details in § 3.3.6.* *Phylaws participated to the EC's meeting on FP7 H2020 discussion 1st march 2016 Brussels (see § 3.3.6.).*
A.5	*It is important that a solid and cohesion concrete actions on standardization bodies are made within the project so it does not end up as a sum of random topics on PHY related security mechanisms.*	*See answers of line C.11 and description of standardization initiatives at § 3.3.3.*
A.6	*Exploitation plans by the project partners are almost non-existent…*	*See answers of line C.12*
A.7	*SWOT analysis of proposed solutions is limited to S/T aspects only, and there are no cost models (present or foreseen) addressing economic viability of the same*	*See answers of line C.10*

A.8	*There is no evidence of an IPR strategy,*	*See answers of line C.12*
A.9	*Reported synergies and collaboration with other FP7 projects are limited.*	*See answers of line A.4*
	Ref: [PHYLAWS_GA-CR_PPR2] § b. Page 6-7	***Phylaws' answers***
B.1	*Deliverable quality :* *The quality of the deliverables should be improved* - *remove typos and grammar errors* - *Remove unnecessary duplications of text and figures (e.g. replace with references)* - *Reduce excessive "wordiness"; for instance, in D4.1, textual presentation of results for equation 4-49 on pages 71-73 (e.g. replace with tables and graphs), and also D2.4 has several grammatical and spelling errors.*	*Deliverable D2.4. was updated by enhancing the introduction part and by correcting its typo and grammar errors. New version V3.0 was published in December 2015* *Deliverable D4.1. was updated by enhancing its introduction part and by removing duplications and replacing long text explanations by synthetic tables and references to figures. New version V2.0 was published in December 2015* *NB : Deliverable D2.1 (threat analysis) was revised in a version V3 hat takes into account new threat scenarios where Eve is informed of subscriber identities and key.*
B.2	*Scientific publication on the web site* *Maintain an up-to-date list of all scientific publications and relevant abstracts on the Publications section of the website.*	*Up-to-date list on the Publications section of the website: done by regular upgrades of the web site: all publications are in line since end Dec 2015.* *Relevant abstracts the web site: to complex and heavy to manage => we "compensate" by giving the complete title of each paper that is usually rather explicit and a direct and fast access to the paper by a single click.*
B.3	*Allow free full paper downloading either on the same website or via a twin website (e.g. VTT's or TPT's). If necessary, use last "accepted" version before final "copyright" formatting (e.g., for IEEE papers). Preferably, indicate name and e-mail of contact.*	*Done at the Phylaws web site by upgrading the page site "publications" (last update 30 December 2015)*
B.4	*Explain the reasons (e.g. in D6.1) for the choice of the MATLAB channel model from QuaDRiGa for the study of the simulator.*	*Done in the revised version of D6.1 V2.0 that includes an annex 8 (especially § 8.1) dedicated to these explanations.*
	Ref: [PHYLAWS_GA-CR_PPR2] § c. Pages >7	***Phylaws' answers***
C.5	*Management / coordination* *Coordination between WP3 and the other WPs. Provide a clear plan as to which of WP3 solutions will be demonstrated.*	*See § 3.3 of this document and the intermediate technical report [PHYLAWS_D.1.3a] prepared for the next technical review meeting (30 March 2016).*
C.6.1	*Reporting* *Provide more detailed information in future reports about novelty.*	*Some of the introductions and parts of the past deliverables were re-written in this sense (see D2.4 version 3.0, D4.1 version 2.0, D6.1 version 2.0). A clarification effort was done for new deliverables of period 3 published recently (D3.2, D4.2 and D4.3).*
C.6.2	*Reporting* *The project still has many technological options and choices to make. Although some of those choices should have already been done during the second reporting period, the reviewers would like to be briefed on the main technological-options decisions and associated rationality at the next review meeting*	*Global answers on technological options for Physec schemes are provided by the standardization strategy (see § 3.3.3) and the "IPR strategy" (see § 3.3.7). In fact, since the start of the project, we oriented the development toward the best chances of industrial exploitation, IPR, and standardization perspectives, but we needed assurances for feasibility proof. As we are now confident about our solutions (end of period 2), we focus now on RATs independent solutions (as most as possible, for largest application cases), and on application scenario to signaling and to first stages of radio access, which are the most difficult in practice (because secure paring and authentication are needed) but the weakest into public RATs (as proven into D2.1).* *Answers dedicating to simulation items are provided in new version V2.0 of D6.1 and complements are present in D6.2 (simulation plan).* *Answers regarding experimental items will be provided in D5.1 and completed into D5.2 (experimental plan).*

C.7.1	*Technical Focus* *There is some degree of fragmentation where individual pieces of work are scattered through studies, simulations and experiments, lacking an integrated perspective.*	*Many "fragmentation" problems were only apparent. In fact they occurred during period 2 as a consequence* - *of first periodic review PPR1 and requirements expressed in [PHYLAWS_GA-CR_PPR1] (rewrite a new DoW during period 2, wait for reviewer expertise and EC acceptation, etc.)* - *of late acceptance of new DoW by EC (10 March 2015 [PHYLAWS_GA-AM1])* - *of completion time of the experimental test bed and simulation.* - *That is why during previous period 2, prior experiments and Physec schemes were developed from partial modeling and experiments provided by the TCS test bed.* - *in order to anticipate (and prepare) WP5 and WP6.* - *In order to provide material for dissemination and standardization.* *Right now, it appears that, thanks to this anticipation of test bed experiments and simulations,* - *a fine understanding of propagation randomness was achieved (see the thesis of Ms. T Mazloum). Note that these academic results were sustained and completed thanks to CIRs outputs of the test bed at real fields Wifi and LTE carrier (see for example the PhD dissertation of Tagrid Mazloum [PHYLAWS_PhDTM] chap 7),* - *the feasibility proofs (even remaining partial) of several major items were assessed, such as reconciliation and privacy amplification into SKG schemes, SC coding capability under radio advantage etc.* *The consortium is now confident about practical perspectives of Physec schemes, that is why patent and standardization were possible at end of year 2015 (see § 3.3.3. and 3.3.7)* *Moreover, this successful approach allowed us to optimize Physec schemes (see for example development of SKG and SC schemes in D4.3). It thus* - *mitigates experimental risk of period 3 and* - *provides convincing materials for dissemination, and to standardization bodies (see § 3.3.3)*
C.7.2	*Technical Focus* *Therefore the project should identify a representative but limited set of target use cases of references…*	*This is done in the standardization strategy and IPR Strategy (see § 3.3.3 and 3.3.7).Our solutions are almost RAT independent (except TDD for "simple" SKG implantation). Whatever is the RAT, our main targets are relevant to the weakest parts of radio access stages:* - *Signaling integrity and confidentiality* - *User Equipment Identity Authentication and confidentiality* - *Subscriber Identity Authentication and confidentiality* - *User data integrity and confidentiality,* *This applies especially to M2M/IoT, LTE and Wifi Aggregation (LWA), radio cell (5G targeted for Standardization), in WLANs, which seem right now the best chances for Standardization (see § 3.3.3).*
C.7.3	*Technical Focus* *… A dedicated chapter should either be added to the next Periodic Report D1.3.a, or included in an appropriate upcoming deliverable (within M39), or added as an appendix update to an existing one.* *In the same chapter, all assumptions and*	*Annex 8 of deliverable D6.1 answers this point regarding simulation* *Such a chapter will be added to deliverables of WP5 regarding experimental feasibility proof.* *Nevertheless, Physec schemes may address all kind of scenarios in radio-communication services, because it essentially targets protection upgrades of sensitive stages of the radio access, by keeping RAT independent (except TDD/FDD). Thus, it is more*

	constraints to be used for proof of concept and demonstration of feasibility of each reference use case, should be explicitly stated, and be consistently referenced (instead of re-stated) across the whole project.	*efficient to target access capabilities encountered whatever is the scenario (such as mentioned above):* - *Signaling integrity and confidentiality* - *User Equipment Identity Authentication and confidentiality* - *Subscriber Identity Authentication and confidentiality* - *User data integrity and confidentiality.*
C8.1	*Technical Topics Recommendations* *Improve the understanding of interplay between physical layer security and classical cryptographic solution.*	*First, it appears the Physec could help existing SIM-based and UIM-based secured protocols such as 3/4G EPS–AKA. Analyses complements on this item can be found into D2.1 V3.0 and into recent publications (ETSI WS – 01/2016).* *Then, from crypto expert of TCS, it appears that Physec has many relationships with quantum cryptography.* *Finally, as initially projected in Phylaws project since its start, the TCS crypto lab will provide during period 3 expertise of the complete Physec protections schemes.*
C.8.2	*Technical Topics Recommendations* *The channel reciprocity assumption should be investigated in more detail.*	*Investigation of this hypothesis has been done from theoretical publication during the state of the art (period 1).* *This has been completed partially (single sense Alice to Bob) during period 2 with the TCS part of the experimental test bed: examination of the space and time coherence of the radio propagation - See deliverables of WP3 and WP4).* *This is recently completed experimentally with the Wifi test Bed (WP5), whose developments shall take into account accurate Tx / Rx receivers calibration in order to assess the assumption. This may have impact on the reconciliation step of SP and SKG (see &3.2.3). D1.3a will focus on this points by showing that reconciliation works practically. Note that these very recent results have just been published in March 2016.*
C.8.3	*Technical Topics Recommendations* *Correlated channels for Bob and Eve should be clearly addressed in terms of the performance limitation of the investigated approaches.*	*Investigation of this hypothesis has been done from theoretical publication during the state of the art (period 1).* *This has been completed partially (single sense Alice to Bob) during period 2 and starting period 3 with the TCS part of the experimental test bed: examination of SKG and SC results at both Bob's and Eve Sides. The trends are very good for space de-correlation: See deliverables of WP3, thesis of Ms. T Mazloum, D4.3 and our recent publications.*
C.8.4	*Technical Topics Recommendations* *Collaborating Eve scenarios with multi-antenna solutions should be more closely integrated in the measurement and test set-ups.*	*Already taken into account by considering* *- several antennas for Eve* *- scenarios where Eve is informed of subscriber identities and keys.* *For scenario updates: see the revised version V3.0 of D2.1 (threat analysis)* *For developments/experiments: see D4.1, D4.2 D4.3.* *For experiments: see D5.1 and D5.2* *For simulations: see D6.1 and D6.2*
C.8.5	*Technical Topics Recommendations* *Additional signaling requirements regarding the integration of PHYSEC into existing protocols should be quantified.*	*Questions about this item occurred during WS and conference presentation.* *Regarding the added signaling at PHY layer, it is a final output of Phylaws. Nevertheless, the current trend are the following:* - *added tag signals are required for secure pairing but they are low DSP and present only at the start of the radio access => no practical increase of spectrum usage, limited added signaling at the Air interface only.* - *when no feedback messages are required , the added signaling for SKG and SC should remain very low.* - *A significant added signaling is required only when feedback messages are required, but such messages are usually weak*

		and they disclose information => the Physec schemes we propose will avoid them. *The strict Physec schemes should not need added signaling in MAC and upper layers.* *Nevertheless the PHY randomness could be propagated into upper protocol layer (input of integrity control or cipher schemes for example). In later case only, the relevant data stream would correspond to generated keys for example meaning a few hundred bits per second at its maximum.*
C.8.6	*Technical Topics Recommendations* *The results of channel measurements should be taken more in account by the other WPs. Import measured channel data to the simulator.* *It would be useful for the next stage to use some of the measured channel data into the channel simulator in the form of 'play back' and compare the results with the channel simulator results from the adopted model*	*The results of channel measurements are taken in account by the other WPs* - *Physec scheme development in WP4 are tested and optimized thanks to channels recorded in WP3* - *WP5 demo will provide capabilities for real field radio communication over the air, and for replay of recorded channels* - *WP6 simulations provide capabilities for propagation models and replay of recorded channels.* *See for more detailed results in [PHYLAWS_D.1.3a]*
C.9	*Dissemination* *Further papers in top conferences and high quality journals should be targeted, and patent applications related with the project outcomes are recommended.*	*Papers in top conferences and high quality journals: several attempts were done during period 2 towards IEEE journals, some were refused because of misunderstanding in the examinations of the topics we proposed. Nevertheless, we were present in ICC, EUCNC, etc.* *Patent applications: Three patents were written and submit to French patent office in December 2015. More explanations can be found in § 3.3.7*
C.10	*Economic dimensions – legacy implications*	*For the moment, we do not know cost/business model or even publication associated with the security of the radio link of public RATs. As this seems a major topic of project 5G-Ensure, the Phylaws consortium expect some highlights from this project during year 2016 and will derive impacts specific to Physec-based security solutions.* *Regarding deployment, legacy implications etc., the best arguments rely to the facility of Physec schemes implantation through software add-ons into nodes and terminals that impact only the PHY layer and not the upper layers.*
C.11	*Standardization strategy* *The project standardization strategy and initiatives need to be reconsidered and more effectively focused, taking into account the limited time available until the end of the project…*	*During the start of period 3, we intensified significantly standardization actions towards ETSI (WS presentation), 3GPP (SA3#82 meeting Dubrovnik), and ITU-R (WP 5D Beijing). Proposals and discussion documents were written and submitted by Phylaws. Phylaws contributes to study Items on security and to reports that are now in preparation at 3 GPP and ITU. See § 3.3.3 for more details.* *Internally, discussion with project relevant to 5G (such as 5G-Ensure) is in progress and common actions are expected. Besides, Phylaws participates to RASR clusters, to H2020/FP7 meeting of EC dealing with the 5GPPP's activity, etc.*
C.12	*IPR strategy* *Potential IPRs need to be identified, and relevant protection (e.g. patenting) and exploitation (e.g. licensing) strategies need to be agreed with adequate advance to avoid loss of opportunities (e.g. if results are published in journals)*	*IPR strategy: Three patents were submitted to French patent office in December 2015: one on Secure pairing, one on Secret Key Generation, one on Secrecy Coding* *Publicity is under authorization by French DGA and acceptation is under the patent French office. If OK, extension policies are prepared and relevant budgets are estimated. More explanations can be found in § 3.3.7.* *The potential use by industrial partners is clear when reading our patent submission, our publications (see for example ETSI*

		Workshop) and our standardization proposals (§ 3.3.3). It relies to better pairing of terminals and nodes for authenticated radio links negotiations and better protections of signaling and access messages in any RAT.
	Intended use by industrial partners of PHYLAWS results (IPR and non-IPR components) need to be convincingly explained in the upcoming Periodic reports 1.3.a and 1.5	*Celeno, as a provider of secure-enhanced Wifi chipset, will directly take benefit of both IPR component (SKG, AN-BF + SC)* *Besides, TCS and VTT are interested in secure-enhanced applications of LTE for various private and military applications. Secure Pairing, SKG and SC (which all will be under IPR) are basic capabilities for such applications.* *Several tracks for re-use of Physec-based security concepts into military radios were presented and discussed at EDA captech 31st meeting which held on 10 Nov 2015 Brussels – see § 3.3.3.3. Unfortunately, military use of Physec-based schemes cannot more be detailed in the context of a public project such as Phylaws. Similar restrictions may apply because of industrial secret regarding professional Radio networks (Note: these restrictions concerns mainly partners TCS and VTT).*
	Ref: [PHYLAWS_GA-CR_PPR3] §1a. Page 2	**Phylaws's answer**
D1	Existence of significant delays in some WPs	This was the main coordination activity of second half of period 3: the main issue was to compensate the late delay of the Wifi test bed development with adaptation of the experimental strategy. A secondary issue was to limit the impact of these dvT delays at other WPs and deliverables and at project organization. In practice, TCS significantly contributed to WP5 validation and deliverable redaction, modified its approach of the security analysis into deliverable D4.5 and D4.6 and adapted his dissemination and standardization strategy by re-using and deepening exploitations of previous signal records performed with the interceptor part of the test bed during period 2 and starting of period 3 of the project. Note that these management issues induced significant added works and costs for partner TCS.
D2	No clear explanation of the nature of unexpected problems in the development of the WiFi test bed of has yet been provided	Explanations ("clear" or not) were given during PPR3. We recall that this late delay of the wifi test bed development is mainly due to bad calibration mismatch compensation in its firmware. Explanations are accurately completed into version 2.1 of D1.3, QMR 1 and QMR2 (parts WP5 and risk analysis) published month 42 and month 45.
D3	Project reporting is definitely not of sufficient quality	TCS recalls that according to the PPR2 outputs the PPR3 should be initially an intermediate technical review, centered on results and not on management issues. Despite this remark, TCS submitted again a completed deliverable D1.3 version V2.1 month 43, which follows all the recommendations expressed by the reviewers about reporting (including especially a completed risk analysis).
	Ref: [PHYLAWS_GA-CR_PPR3] §1b. Page 3	**Phylaws's answer**
D4	Improvement and resubmission of PPR3 (deliverable D1.3)	Done in two phases: Version V2.0 in April 2016 (3 weeks after RM3) with a new title, a section about use of resource, a completed section on Risk Management, completed description of work done and of main results achieved in the period regardless of whether they are already covered by submitted deliverables, summary of ongoing and future work, summary of outstanding critical issues, contents revised according to the time of submission, etc. Version V2.1 was completed with news informations about test bed and risk management strategy.
	Ref: [PHYLAWS_GA-CR_PPR3] §1c. Page 4	**Phylaws's answer**
D5	All recommendations from this and previous Reviews on the structure and content of Project	The redaction way above was also applied to QMR1 and QMR 2 (in a shortened way) and to present deliverable D1.5.

	Periodic Reports also apply to the Final one (PPR4)	
D6	Quarterly Management Reports, different from Project Periodic Reports, should be produced at the end of each remaining project Quarter.	QMR1 and QMR2 were delivered on time, even if QMR1 was slightly upgraded Month 45 to better match with the reporting included into QMR2. QMR3 was cancelled, because its release occurred to late compared to the end of the project, while the Phylaws team was very busy with the final Workshop and final concretization of standardization actions.
D7	Quality of deliverables	An effort is continuously applied, regular improvements and completions of deliverable lead to updated versions on the web site
D8	Finalization and submission of P3 deliverables by M48	The Phylaws partners made a tremendous effort for achieving most of technical deliverables before the end of the project. Most of them were completed with significant content and delivered before the 18th of November (Month 48.6).
D9	Cooperation between WPs and between the involved research groups should be further reinforced	During first half of period 3: prepared and partially achieved with project Duplo. during the second half of period 3: achieved with 5G –Ensure project, French and foreign industrial + administrations at standardization bodies
D10	Functional proof-of-concept should be provided by the end of the project	Achieved at the final Work shop of the project (PIMRC' 2016), also in latest deliverables of WP4, with completions into WP6 D6.3 (simulation results), WP3 D3.5 (massive exploitation of CSI records that sustain the security analysis), final deliverables D5.3 D5.4 D5.5 of WP5 (reports on experiments with the Wifi test bed).
D11	WRC15 has identified a number of frequencies in the higher bands between 24-86 GHz as candidates for future wireless networks. While the test beds developed in this project targeted the lower frequency bands below 6 GHz, it would be useful to identify how the work presented here relates to 5G.	Done through our standardization proposals (see Deliverable D1.8 for a complete overview). For example AN-BF + SC directly applies to massive MIMO hardware into 5G.
D12	The Advisory Board's suggestions to develop specific business cases, and to find supporters not only among suppliers, but also from customers, should certainly be pursued.	Done when occasion occurred through our contacts in standardization bodies and through our standardization proposals (see Deliverable D1.11 for a complete overview).
	Ref: [PHYLAWS_GA-CR_PPR3] §2a Page 6	**Phylaws's answer**
E.1	Regarding this, it is of further concern that no serious investigation of the problem has taken place yet, and that no corrective actions have been identified and activated	We contest this interpretation. Maybe our explanations were not clear enough for the reviewers, but the wifi test bed problems were already investigated and understood (see above). Implementation of a suitable corrective solution took time to partner CEL and occurred most of the test bed and WP5 delays.
E.2	Lack of any related information on actual resource usage in the period, also makes it impossible to determine to which extent the problem could lie in the (insufficient) amount of effort used (in particular by CEL) and if any margins for recovery actually exist.	This information was provided in the upgraded version 2.0 and 2.1 of deliverable D1.3 and then in QMR 1 and QMR2, all published a short time after PPR3/RM3.
	Ref: [PHYLAWS_GA-CR_PPR3] §2b Page > 7	**Phylaws's answer**
E.3	Nevertheless, project management itself (T1.1) is definitely not up to expectations.	See D3. TCS recall that the PPR3 was an intermediate technical review, centered on results and neither on management issues nor on cost issues. Despite this remark, TCS submitted a completed deliverable D1.3 version V2.1 month 43, which follows all the recommendations expressed by the reviewers (including especially a completed risk analysis).
E.4	The submission title of PPR3 ("Quaterly Month Report 1") is not correct. It should be taken into due consideration that nature, purpose and content of the various types of periodic reporting documents usually required in FP/H2020 Projects (that	Corrected in D1.3 version 2.0 and 2.1, and into QMR 1version 2.1 and QMR2 version 1.0. Nevertheless TCS points out that PPR and QMR templates are not very clear about their content and full of bugs in their style management. This does not help for clear redaction.

	isPPRs and QMRs) is intrinsically different and only partly overlapping.	
E.5	D4.5 is significantly delayed because of slow progress in WP5, which also affects the future submission of D4.4 and D4.6. Official end date of WP4 is M46. D4.5 is delayed because of its dependence on D3.4 and D5.3, both of which are late too and at this time available in Draft version only. Furthermore, no anticipation of its content and relevant achievements is provided in PPR3.	In practice, it is a dream to think that all can be anticipated. In fact, consideration at month 44 that interception experiments with the Wifi test bed were more possible because of the processing development delay of the attacks, TCS had to refund the strategy of the security analysis. This was achieved in both deliverables D4.5 and D4.6 delivered M48. Otherwise, deliverable D4.4 was late only because TCS focused its time and energy first on other priority during summer 2016: - To help CEL (validation of the Wifi test bed through SKG results, radio analysis of calibration problems) - To finalize preparation of WS, write journal paper s, book chapters and standardization proposals. Only after, D4.4 was achieved (end of M46)
E.6	Eve interception investigation will be carried out in the 2.4 GHz band (material constraints). The studies about resilience of the proposed schemes to attacks will only start in June and will be done in Paris, jointly with TCS crypto-team	Due to excessive delays in the test bed development, TCS changed its strategy for the resilience+security analysis (still performed by radio + crypto experts) and avoided interception experiments, as mentioned in QMR2 (risk analysis)
E.7	Although some of the delays experienced in WP5 are acknowledged and reported in PPR3, no adequate explanation or justification has been provided.	Yes explanation or justification has been provided (maybe not clear enough). It is clear in the project building that D3.4 and D3.5 are highly dependent on the Wifi test bed outputs.
E.8	Moreover, no explicit assessment has been made of implications on current and future work, in this and other WPs, no criticality is reported, and no mitigation measures have been envisaged and put into place	Yes. See above. Nevertheless in March 2016 it was not clear whether CEL could overcome calibration difficulties. Finally, with some added help and development, CEL partially succeeded at the end of the project. Risk analyses were also completed following the history of the test bed development into PPR3 version 2.1, QMR1 and QMR2. Finally, while long duration dual sense calibrated CSI records were available only Month 48, redaction of D3.4 and D3.5 thus could start only M 47. Meanwhile, all previous available records have been exploited as most as possible in WP4 (resilience and security analyses), in first deliverables of WP3, in publications and in standardization proposals. Completed CSI records, when available confirmed the previous results and analyses with better estimates of Physec schemes performance, of joint entropies and mutual information of legitimate and attacker propagation channels.

Figure 9: Actions and answers to the remarks recommendations and requirements of reviewers and EC (PPR2 Brussels 9/09/2015, PPR3 Brussels 30/03/2016)

3- Detail of work performed during period 3

Preliminary note for an easier reading of this section 3.

- *In italic characters: text common with previous documents [PHYLAWS_D.1.3_PPR3] relevant to first half of period 3 (*M33- M39*) recalled here for a complete overview of period 3 activities.*
- In normal characters: new text relevant to second half of period 3 (M40-M48).

3.1- General

According to the Action Plan [PHYLAWS_GA-AC], the revised Description of Work ([PHYLAWS_GA-DOW2]) and the advice of reviewers during the PPR2 [PHYLAWS_GA-CR_PPR2], the work of period 3 (month 33-48) concerned all Work Packages except WP2 and mainly:

- Work package 1, with a very intensive effort on the following activities to perfectly achieve the objectives, despite their inherent difficulties:
  - Advisory board (Task T1.4) : second meeting and associated report D1.13 [PHYLAWS_D1.13], third meeting cancelled, final synthesis report D1.14 [PHYLAWS_D1.14]
  - Standardization activities (Task T1.3): intense activity at 3GPPP and ITU, deliverables D1.10 [PHYLAWS_D1.10] and D1.11 [PHYLAWS_D1.11].
  - Continuous dissemination activities (Task T1.2) in order to sustain standardization initiatives and enhance the impact of the project. Numerous publications into two ETSI workshops, into Wincomm forums etc., redaction of paper journals and book chapters. Organization of the final Workshop of the project hosted by PIMRC'2016 Valencia Spain Sunday (4th September 2016), etc. redaction of deliverable D1.8 [PHYLAWS_D1.8].
  - Management activities, especially in the second half of period 3 to compensate the late achievement of the Wifi test bed into WP5 and to mitigate the impact on other WPs, at deliverable furniture, and also at project organization. Redaction of numerous management deliverables [PHYLAWS_D1.3], [PHYLAWS_D1.3_PPR3], [PHYLAWS_D1.3_qmr1], [PHYLAWS_D1.3_qmr2], [PHYLAWS_D1.4], [PHYLAWS_D1.5].

- *End of academic work into work package WP 3, leading to the delivery of D3.2 concluding task T3.1, of D3.3 concluding task T3.2. In addition, note that academic works of WP3 led to many publications (see § 3.3.5* and deliverable D1.8 [PHYLAWS_D1.8])
  - *Analysis of the performance of SKG schemes in relation with the channel richness and the propagation environment*
  - *Publications relevant to recent progress in SKG experiments, in the framework of the thesis of Ms. Taghrid Mazloum.*
  - *Publications relevant to recent progress in the design of secrecy codes.*
  - *Defense of her thesis by Ms. Taghrid Mazloum, that held recently in Telecom Paris Tech (12 February 2016). Note that these academic results were sustained and completed thanks to CIRs outputs of the test bed at real fields Wifi and LTE carrier (see for example the PhD dissertation of Tagrid Mazloum [PHYLAWS_PhDTM] chap 7)*
  - *Joined publications between academic and industrial partners relevant to experimental results in CIR extraction and in SKG experimental results, highlighting their practical perspectives for secrecy.*

- Continuation and end of experimental investigations of radio-channel into work package WP3:
  - While only a draft version of D3.4 [PHYLAWS_D3.4] relevant to task T3.3 could be published in March 2016, D3.4 was updated and completed in November 2016 after finalization of the developments of the Wifi test-bed in WP5. It now includes reporting on intensive propagation measurements over the 5 GHz and the 2.4 frequency ranges - real field over the air propagation).
  - Redaction of deliverable D3.5 [PHYLAWS_D3.5] (with the same constraints as D3.4 above). D3.5 exploits the long duration dual sense CSI for SKG enhanced evaluation, accurate estimations of entropy and mutual information at legitimates and attackers, which input the security analysis and confirmed the good resilience and security trends of Physec-based secure schemes highlighted in algorithm studies of WP4.

- Continuation and end of Work package 4:

  During the first half of period 3:
  - *the delivery of D4.2 [PHYLAWS_D4.2] concluding task T4.1 (transec schemes based on Physec concepts)*
  - *the delivery of D4.3 [PHYLAWS_D4.3] relevant to task T4.2 (netsec schemes based on Physec concepts)*

  During the second half of period 3:
  - the delivery of D4.4 [PHYLAWS_D4.4] ending task T4.2
  - the delivery of D4.5 [PHYLAWS_D4.5] and D4.6 [PHYLAWS_D4.6] relevant to task T4.3 (improvement of security of the radio links within existing and future RATs, radio resilience analysis and crypto security analysis of Physec-based schemes when facing nominal attackers and ultimate attackers, synthesis of the technical content of our standardization proposals).

  We recall that

  - *Task T4.1 of WP4 concentrated on means to provide a secure pairing and a radio advantage to the legitimate link,*
    - *first at the earliest stages of negotiation (transmission of channel sounding signal probes, protocol for Channel State Information, device authentication, subscriber identification, ciphering negotiation etc.), thus preventing attacks at the communication starting,*
    - *then at on-going communications.*

    It focuses mainly on Tag Signals and Interrogation and Acknowledgement sequences (object of our first patent [PHYLAWS_Patent1]).

  - Task T4.2 deals with implantation of complete Secret Key Generation and Secrecy coding schemes by remaining realistic and practical.
    - D4.3 explicates first attempts for implementing and simulating Secret Key Generation and Secrecy Coding with very promising results.
    - D4.4 deepens the performance with exploitation simulation and first real field records, then proposes and tests several algorithm optimizations.

    Task T4.2 focuses mainly on SK and SC schemes (object of our second and third patents [PHYLAWS_Patent2] [PHYLAWS_Patent3]).

  - Task T4.3 deals with implantation perspectives of Physec-based concepts (studied in previous tasks T4.1 and T4.2) into existing and future RATs in the following way:
    - Analyses of the radio resilience of Physec-based implementations into existing RATs when facing attacker at the physical layer (passive and active), nominal and ultimate), performed by radio experts of TCS. Optimization proposals. Highlight of performance when facing nominal threats. Highlight of limitations when facing ultimate threats.
    - Analyses of the crypto security of SKG and SC implementations, performed by crypto experts of TCS. Key-free enhancement proposals derived from crypto skills.

  - All these tasks were input by the study results of WP3 issued from the intense collaboration of academic and industrial partners of the consortium.

  - Outputs of WP4 have driven both experimental and simulation development by providing algorithms, Matlab codes, elements of feasibility proof for validation purposes, which were directly implanted into Wifi test bed (WP5) and LTE simulator (WP6).

  - Most of our publications and standardization proposals during period 3 concern the innovative security concepts which were developed and patented into WP4, the completion of feasibility proofs being achieved into WP5 and WP6 and enhanced by the latest works of WP3 T3.4 (Deliverable D3.5), which confirmed previous evaluations of joint entropy and mutual information of legitimate and attacker propagation channels.

- Continuation and end of work package 5 (which started period 1, but provided its deliverables at the beginning of period 3),

  During the first half of period 3:

  - *Firmware development of the test bed.*
  - *Premium dual sense CIR extractions under Wifi Carriers, which led to our first Key Generation at 5 GHz 802.11 ac links with the complete enabling of the reconciliation and amplification scheme at both Alice and Bob's side.*
  - *Publication of deliverable D5.1 [PHYLAWS_D5.1], in March 2016 (test bed architecture.*
  - *Publication of deliverable D5.2 [PHYLAWS_D5.2] in March 2016 (experimental plan).*
  - *Publication of deliverable D5.3 [PHYLAWS_D5.3] in March 2016 in draft version (first experimental results with the test bed).*

  During the second half of period 3:

  - Processing and (partial) resolution of calibration issues with off-line post processing of dual sense CSI records.
  - Implementation of software Matlab codes output by WP4 and relevant to SKG and SC schemes.
  - Adaptation of the experimental plan to the restricted remaining time: massive dual sense CSI records were performed in CEL apartment (e.g. Israel) only, and no more in France. No more interception experiments were planned with the TCS test bed (no time enough for attacks' developments and tests), Eve being modeled by other Wifi test bed instances, or single antenna receiver and recorder with analyses capabilities (wireshark software).
  - Short duration time dual sense CSI records (start of summer 2016) and then long time duration dual sense CSI records (end of summer 2016) - exploitation with SKG codes issued from WP4 – enabling of AN-BF situation and exploitation within SC codes issued from WP4.
  - Invited paper at the Phylaws final Workshop hosted in PIMRC'2016, which presented the experimental results and performed read time demos of the test Bed (with embedded SKG and AN-BF+SC).
  - Contribution to the journal papers and book chapters with the WP5 outputs.
  - Publication of final version of Deliverable D5.3 [PHYLAWS_D5.3] (December 2016).
  - Redaction and publication Deliverable D5.4 [PHYLAWS_D5.4] (December 2016).
  - Redaction and publication Deliverable D5.5 [PHYLAWS_D5.51] (December 2016).

- Continuation and end of work package 6 (which started period 1, but provides its deliverables at the beginning of period 3),

  During the first half of period 3:

  - *Achievement of the first task T6.1 of work package 6, leading to the publication of an updated version of deliverable D6.1 [PHYLAWS_D6.1] which deals with the specifications of the LTE simulator, provided propagation scenarios and precised additional developments in progress in the simulation of LTE links in order to model and implant Physec-based security solutions.*
  - *Achievement of the second task T6.2 of work package 6, leading to*

    - *Implementation of Software codes output by WP4 and relevant to tag signal processing, SKG schemes, and SC schemes were into link level simulator and tested*
    - *First Simulation results for the LTE link level performance of the LTE waveform signals with and without underlying tag signals.*
    - *First simulation results of SKG schemes and relevant analyses of performance.*

During the second half of period 3:

- Publication of deliverable D6.2 [PHYLAWS_D6.2] (April 2016) which describes simulation plan, simulation scenarios and presents first simulation results).

- Achievement of the third task T6.3 of work package 6, leading to:
  - Validation of the LTE link level simulator with Physec-based security schemes
  - Complete simulation results for the LTE link level performance of the LTE waveform signals with and without underlying tag signals
  - Complete simulation results of SKG schemes and relevant analyses of performance
  - Complete simulation results of AN-BF + SC schemes and relevant analyses of performance

- Invited paper at the Phylaws final Workshop hosted in PIMRC'2016, which presented the simulation results relevant to Secure pairing (TS and IAS), SKG and AN-BF+SC.

- Contribution to the journal papers and book chapters with the WP6 outputs

- Publication of deliverable D6.3 [PHYLAWS_D6.3] (September 2016) which provides complete simulation results and derives recommendation for standardization.

3.2- Work package 1 (Management, Dissemination, Standardization, Advisory Board) and technical work packages 2 to 6

3.2.1- Task T1.1 - Management

3.2.1.1- Overview

The management effort was very intensive during period 3. The main achievements are described in section § 2.3 – H section and in § 3.1 above. In addition one has to recall the following "daily" actions:

- Preparation of the Second Periodic review held in Brussels 09 September 2015 including redaction and publication of deliverable D1.3 [PHYLAWS_D.1.3].

- Preparation of the intermediate third Periodic review held in Brussels 30 March 2016 including redaction and publication of deliverable D1.3a [PHYLAWS_D.1.3_PPR3].

  - 3 face to face technical meetings, one held 10 September 2015 in Brussels, one held the 21st January 2016 in Paris, one held the 31st March 2016 in Brussels.

- Following of IPR issues: defense of the 3 patent projects submitted to the French patent office

- Organization of Advisory board accommodations and social event (held 19 January 2016).

- Organization of mission accommodations for our numerous standardization actions (ETSI WS, 3GPP SA3#82 to SA#86, 4 sessions ITU-R WP 5D etc.).

- Discussions with other funded projects dealing with 4G, IoT, 5G (Duplo, Prophylaxe, 5G-Ensure, Sonata, Coherent).

- Redaction of deliverables D1.1 [PHYLAWS_D1.1], D1.2 [PHYLAWS_D1.2], D1.3 [PHYLAWS_D1.3], D1.3a [PHYLAWS_D1.3_PPR3], D1.5 [PHYLAWS_D1.5], D1.4 [PHYLAWS_D1.4], revised version of DOW [PHYLAWS_GA-DOW2], added action plan, added Quarterly Management Reports, added technical review meeting, numerous letters, etc.

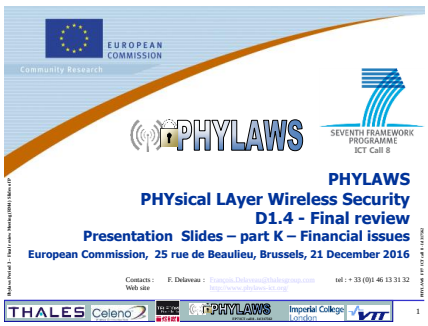
- Review of deliverables before publication.

Despite the numerous difficulties encountered during the project (staff and material missing during period 1, rewritten DoW between period 1 and 2, test bed development delay during period 3, added management reports due to EC requirements, added intermediate technical review meeting, etc.), that involved recurrent updates of experimental planning, searching for alternate solutions relevant to material purchase, staff recruitment, test bed development and test, resilience and security analyses, etc., management and coordination were held very accurately during the project.

At the end, the final results of WP1 Task 1.1 are perfectly in line with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and with the objectives and needs of the project. The price paid by the coordinator for this is significant (roughly added 10 MM work all over the project): see tables of § 3.5.

3.2.1.2- Detail for the period3

See the attached presentation slides above [PHYLAWS_D.1.4_PPR4slides] part K



3.2.2- Task T1.2 – Dissemination

3.2.2.1- Overview

The dissemination effort was very intensive during period 3 especially with the submission and then the organization of the project's Workshop hosted by PIMRC'2016 Valencia.

The main achievements of dissemination during period 3 are described in section § 2.3 – E, all details being included into deliverables D1.6 to D1.8 [PHYLAWS_D1.8] that are shortly described hereafter

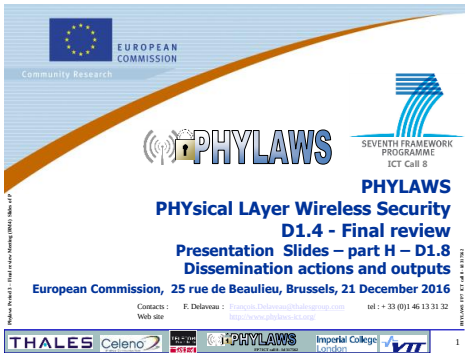
Deliverable	Date	*"Title"* Summary of the content
D1.6	*Period 1* *V1 date 2013-01-31*	*"PHYLAWS Dissemination Plan".* *Includes the planed dissemination actions over the complete project duration*
D1.7	*Period 2* *V1 2015-05-12*	*"PHYLAWS Dissemination intermediate Report"* *Reviews all dissemination actions of periods 1 and 2 of the project.* *Upgrades the planed dissemination actions over the end of period 2 and over period 3, especially linked to standardization actions*
D1.8	Period 3 V1: 2016-10-31	*"PHYLAWS Dissemination final report"* Reviews all dissemination actions of periods 1, 2 and 3 of the project, with a special focus on the final WS, and explanation of the overall significant impact of this (very) successful task of the PHYWS project.

Figure 10: Deliverables of dissemination task T1.2

At the end of the project, dissemination results largely overtake the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and the objectives and needs of the project. The Phylaws consortium hopes that this effort will develop the use of physical layer security in future applied research.

3.2.2.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.4_PPR4slides] part H.



3.2.3- Task T1.3 - Standardization

3.2.3.1- Overview

All our standardization initiatives were sustained by dissemination, especially papers and presentations including experimental results on realistic test cases: shortened and simplified versions of these papers and presentations were the root of most our standardization proposals.

The standardization effort was very intensive during period 3 with numerous meetings in 3GPP SA3 and in ITU WG 5D meetings, leading at the end to agreed proposals from the Phylaws team for 5G standardization evolutions.

The main achievements of standardization during period 3 are described in section § 2.3 – F, all details being included into deliverables D1.9 to D1.11 [PHYLAWS_D1.11] that are shortly described hereafter

Deliverable	Date	*"Title"* Summary of the content
D1.9	*Period 1* *V1 2013-01-31*	*"PHYLAWS Standardization Plan".* *Includes the possible standardization actions considered during the complete project duration*
D1.10	*Period 2* *V1 2015-05-30*	*"PHYLAWS Standardization intermediate Report"* *Reviews the first standardization initiatives held at the end of the period 2 of the project (when first experimental results and elements of feasibility were available)* *Updates the pertinent standardization actions (by following advice of our advisory board) ant he best standardization bodies to be targeted during period 3.*
D1.11	Period 3 V1 2016-10-31.	*"PHYLAWS Standardization final report"* Reviews the all standardization initiatives and results held during period 2 and 3 of the project.

Figure 11: Deliverables of standardization task T1.3

Standardization results are perfectly in line with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and with the objectives of the project.

3.2.3.2- Detail for the period3

See the attached presentation slides below [PHYLAWS_D.1.4_PPR4slides] part G

3.2.4- Task T1.4 - Advisory board

3.2.4.1- Overview

The second advisory board meeting was organized in TPT 20 January 2016. The meeting was hosted in Telecom Paris Tech.

The relevant presentation and minutes of the AB meeting built the deliverable D1.13 [PHYLAWS_D1.13] that has been published in February 2016.

As explained into section § 2.3 – G, a third Advisory Board meeting, initially planned into the Phylaws workshop at PIMC'2016, had to be cancelled, because of the restricted time duration of the workshop.

It is noticeable that Advisory Board advice oriented some of our technical developments and almost all of our standardization initiatives, and this with a personal implication of some of our AB members.

The main achievements of Advisory Board during period 3 are described in section § 2.3 – G, all details being included into deliverables D1.13 [PHYLAWS_D1.13] and D1.14 [PHYLAWS_D1.14] that are shortly described hereafter.

Delive rable	Date	*"Title"* Summary of the content
D1.12	*Period 1* *V1 2013-11-08*	*"PHYLAWS Advisory Board Meeting report".* *Includes the minutes of the first AB Meeting and details how the Phylaws consortium intend to exploit and apply the advice and recommendation of AB members*
D1.13	*Period 3* *V1 2016-02-14.*	*"PHYLAWS Advisory Board Meeting Report"* *Includes the minutes of the second AB Meeting and details how the Phylaws consortium intend to exploit and apply the advice and recommendation of AB members*
D1.14	Period 3 V1 2016-10-31.	*"PHYLAWS Advisory Board final report"* Syntheses the outputs of the two AB Meetings and details how the Phylaws consortium has exploited and applied the advice and recommendations of AB members

Figure 12: Deliverables of standardization task T1.4

Advisory Board actions are in line with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and with the objectives and needs of the project.

3.2.4.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.4_PPR4slides] part I.

3.2.5- Technical work package 2 - State of The Art

3.2.5.1- Overview

WP3 Leader: TCS - Start: Month 1 - End: Month 20 - deliverable list recalled in annex 2.

This work package ended during period 2 and does not concern period 3. It was in line with the initial Grant agreement, initialand revised DoW [PHYLAWS_GA-DOW1] [PHYLAWS_GA-DOW2] and planning. Nevertheless, following the recommendations of the reviewers during last PPR2 [PHYLAWS_GA-CR_PPR2], a new version V3.0 of deliverable D2.4 [PHYLAWS_D2.4] was uploaded in December 2015 that enhances the introduction part and corrects typo and grammar errors. Table below recall the achievements of this work package.

Delive rable	*Date*	*"Title"* *Summary of the content*
D2.1	*Period 1 -> 3* *V2: 2015-12-30*	*"Privacy threats for the radio interface of public wireless networks".* *See [PHYLAWS_D.1.3] for the main content. New version V2.0 includes description of enhanced new attacks where Eve is informed of subscriber identities and key.*
D2.2	*Period 1* *V1: 2013-09-23*	*"Secure architectures and protocols for privacy enhancement of radio terminals"* *See [PHYLAWS_D.1.3] for the content description.*
D2.3	*Period 1* *V1: 2013-11-14*	*"State of the art of physical layer security"* *See [PHYLAWS_D.1.3] for the content description.*
D2.4	*Period 2 -> 3* *V3: 2015-11-30*	*"New opportunities provided by modern waveforms, new security protocols and sensing of radio environments"* *See [PHYLAWS_D.1.3] for the content description. This version V3 enhances the introduction part and corrects typo and grammar errors.*

Figure 13: Deliverables of WP2

3.2.5.2- Detail for the period3

WP2 was ended during period 2.

3.2.6- Technical Work Package 3 - Radio-channel aspects of Physical layer Security

3.2.6.1- Overview

WP3 Leader: TPT - Start: Month 1 - End: Month 42 - deliverable list recalled in annex 2.

While deliverables D3.1 [PHYLAWS_D3.1], D3.2 [PHYLAWS_D3.2] and D3.3 [PHYLAWS_D3.31] were achieved on time, the experimental work of WP3 on WiFi signals to be achieved at the beginning of period 3 was late compared to the revised description of work of the Phylaws project [PHYLAWS_GA-DOW2] and with the relevant planning. The reason was the difficulties for the firmware development and calibrations issues (see § 3.3.9 “risk management”).

Thus, only a partial version V1 of deliverable D3.4 [PHYLAWS_D3.4] could be achieved in March 2016, which was completed in November 2016 by completed version V2.

Deliverable D3.5 [PHYLAWS_D3.5] exploiting the Wifi CSI records of D3.4 was achieved in December 2016.

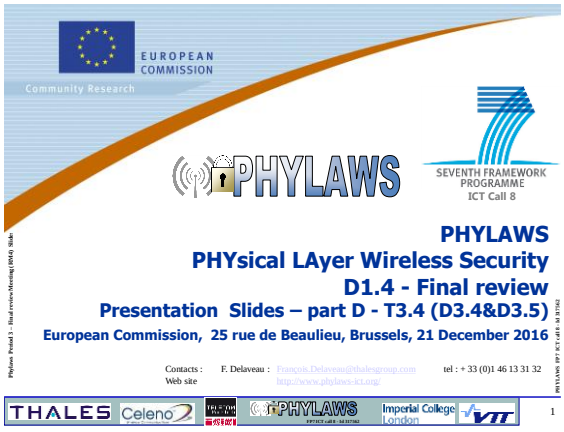
Except this delay, none of this deliverable suffered of the late achievement of the wifi test bed. Their content is complete and full of new measurement results that complete the achievement of the feasibility proof of the patented secure schemes.

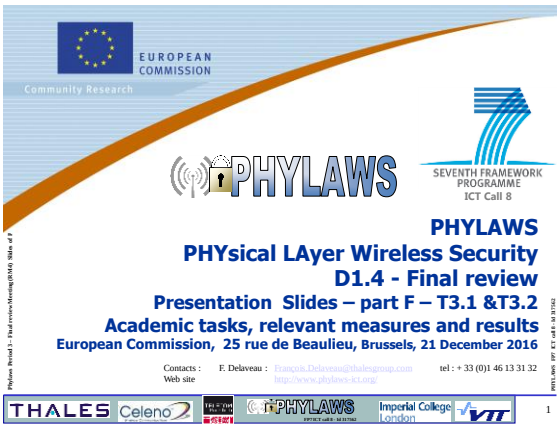
The table hereafter summarizes their contents.

Finally, despite some delays in the WP3 achievement, at the end of the project, WP3 results are perfectly in line with the goals and needs of the PHYLAWS project and with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2].

3.2.6.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.4_PPR4slides] parts D and F.





Deliverable	Date	*"Title"* Summary of the content
D3.1	*V1: 2014-03-10*	*"Channel based random generators: interim report"* *See [PHYLAWS_D.1.3] for the content description.*
D3.2	*V1: 2015-11-30*	*"Channel based random generators: final report".* *This deliverable concludes task T3.1 on channels and SKG, with outputs intended to impact downstream work in work packages WP4, WP5 and WP6. It deals with* • *Evaluation of the performance of the SKG schemes, with a specific focus on the description of suitable metrics.* • *Modeling of non-stationary statistical channel with random distribution of scatterers, by introducing time varying shadow fading effects, then focusing on the improved performance of SKG schemes in this more realistic propagation.* • *Physical interpretation of performance of extracted secret keys, from a simplified variant of dispersive channel model.* • *Radio channel modeling by ray-tracing, carried out in a few environments inside and close to Paris city (France).* • *Radio channel measurements performed through several indoor and outdoor/indoor campaigns and on their first exploitation as input to SKG schemes.*
D3.3	*V1: 2015-11-05*	*"Coding techniques and algorithms for secrecy coding and secret key generation".* *This deliverable first introduces several notions relevant to information theory and the main principle that are relevant to wiretap coding at the physical layer. From a state of the current researches, several wiretap coding solutions are highlighted, especially* • *the wiretap coding scheme for discrete channels, based on the famous LDPC codes and the recently proposed polar codes.* • *extension of the coset wiretap coding scheme to continuous Gaussian channels, by constructing polar lattices* *Secondly, The deliverable deals with practical implantation perspectives of secret key generation in existing and future radio-networks (secret key generation from Gaussian source, using the lattice hashing technique), as stand-alone added modules operating at the physical player, or as added algorithm combined with classical solutions such as TRANSEC, NETSEC and COMSEC protections. It highlights the major channel issues regarding SKG and routes towards the development of channel models and the way to conduct channel measurements or channel simulations suited to the PHYLAWS needs for SKG.*
D3.4	Partial version V1: 2016-03-30 V2 2016-11-21	*"CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band".* The final version of deliverable D3.4 provides • completed details about material and processing into the Wifi measurement campaign at 2.4 and 5 GHz, including calibration issues encountered and partially solved by partner CEL • completed measurement results for dual sense CSI under 5GHz and 2.4 GHz wifi carriers • completed analyses of wifi radio channels issues for an usage in Physec-based secure schemes • numerous illustrations of calibration issues • numerous illustrations of CSI measurements
D3.5	V1.0 2016-11-30	*"Simulations report of PHYSEC methods using measured CIR""* Deliverable D3.5 performs • massive usage of CSI measurements provided by D3.4 for SKG processing, for join entropy estimations, for mutual information estimations • numerous illustrations of SKG results. • complete analyses of the channel randomness properties and their usage for SKG • few exploitations and analyses of the measurements in simplified simulations of Secure Pairing with Tag Signals (modeling and simulation of a complete Interrogation and Acknowledgement Sequence).

Figure 14: Deliverables of WP3

3.2.7- Technical Work Package 4 - Introducing radio-channel randomness in existing and future RATs

3.2.7.1- Overview

WP4 Leader: TCS - Start: Month 25 - End: Month 46 - deliverable list recalled in annex 2.

Recall that this work package really started during period 2.

The work of WP4 achieved during period 3 had to be increased with respect of the revised description of work of the Phylaws project [PHYLAWS_GA-DOW2] and the relevant planning.

- *Deliverable D4.1 [PHYLAWS_D4.1] was achieved on time. Recall that following the recommendations of the reviewers during last PPR2, a new version V2.0. of Deliverable D4.1 (initially delivered period 2) was uploaded which mitigates redundancies of the first version.*

- *Deliverables D4.2 [PHYLAWS_D4.2] and D4.3 [PHYLAWS_D4.3] were achieved on time.*

- D.4.4 [PHYLAWS_D4.4] was slightly delayed according to the new planning issued from PPR3, because of the mobilisation of the TCS team on other priorities:
  - First to support the wifi test validation, by exploiting its own CSI (first partial over short time duration, finally completed over longer time duration) to develop the SKG processing (already validated by re-using CIRs and signals records of period 2).
  - Then to organize and realize the final project workshop, to prepare the relevant papers (including the invited paper on Wifi experiments presented by partner CEL).
  - Third, to write the book chapters and the journal papers (achievement of WP1 task T1.2).

- D4.5 [PHYLAWS_D4.54] and D4.6 [PHYLAWS_D4.6] including radio resilience analysis and crypto security analyses were also slightly delayed (M 48):
  - First, for the same reasons as D4.4.
  - Then, because the study on radio resilience and crypto security of our Physec-based schemes had to be modified, due to the late availability of the massive dual sense CSI records (outputs of T5.3). For more details, see risk analyses and corrective actions into § 3.3.9).

Note that all WP4 activities had initially strong relationship with WP3:

- Algorithm development was first input by results of tasks T3.1 and T3.2.

- Algorithm validation should have been input by results of tasks T3.3 and T3.4 and experiments of WP5 T5.3.

In practice, due to the late availability of WP5 outputs, it was necessary to refund the lead of algorithm development and of the security analysis. Finally, a “reverse sense” applied at inputs and outputs among all these tasks:

- First, thanks to single sense CIR recorded during period 2 and 3 of the project with the TCS interceptor part of the test bed (WP3 T3.1 and T3.2),
  - WP4 managed to validate and optimize most of SKG and SC processing
  - WP4 started the radio resilience and crypto security analysis

- Then, with the few first dual sense experimental CSI available at the middle of period 3 (outputs of T5.1 and T5.2):
  - WP4 completed the validation and optimization of SKG processing (reciprocity restoration issues and reconciliation issues).

- WP4 completed (as much as possible) the security analyses with rough estimations of entropy (min-entropy in practice) and (max and min) mutual information at legitimate and attacker side.

- Finally, when the massive dual sense experimental CSI were produced by the Wifi test bed (T5.3), the relevant analyses performed in task T3.4 and T3.5 (e.g. new estimations of entropy and mutual information for the elaboration of D3.5, now base on long time duration records and large number of samples) confirmed the conclusions of our security analyses (included into D4.5 and D4.6).

Moreover WP4 results largely input

- WP5 tasks (delivery of validated algorithm, validated measurement scenarios),

- WP1 tasks T1.2 and T1.3 (prior results for papers, book chapters, standardization proposals).

The table hereafter summarizes the contents of WP4 deliverables.

Del.	Date	*"Title"* Summary of the content
D4.1	*V1: 2015-06-12* *V2: 2015-12-30*	*"TRANSEC upgrades of existing RATs – study report".* *See [PHYLAWS_D.1.3] for the content description.* *This new version enhances the introduction part, removes duplications and "wordiness" by replacing some long text explanations by synthetic tables and references to figures.*
D4.2	*V1: 2015-11-30*	*"TRANSEC upgrades of existing RATs –analyses and simulation complements".* *Completing deliverable D4.1, the results of this deliverable strengthen the proof of concept of Tag Signals and Interrogation and Acknowledgement Sequences with additional simulations and experiments. In addition, we propose a schemes for building large sets of Tags Signals, we complete the analyses of resilience of the scheme and we definitely conclude on the "tremendous" perspectives of the proposed TS and IAS schemes concerning* - *Enhanced Secure Pairing of devices and most accurate CSI measurements for initiating artificial noise, beam forming, SKG and SC.* - *SINR measurement for controlling the radio advantage directly provided by Tag Signals or by other methods (such as Artificial Noise and Beam Forming) and support further users' attach, identity authentication, cipher key negotiation.*
D4.3	*V1: 2015-11-30*	*"NETSEC upgrades of existing RATs – Study report".* *This deliverable surveys opportunities for Netsec (Network Security) improvements in existing public wireless standards by exploiting channel randomness. It focuses mainly on the following items:* - *New developments relevant to the complete "pre-industrial" implementation of the patented Secret Key Generation scheme (SKG) based on full CSI.* - *An innovative implantation scheme of Secrecy Coding (SC), invented and studied and patented by the Phylaws team. Even if it may be suboptimal regarding the secrecy capacity, this new scheme allows a practical implementation within node and terminal by using well-known coding components of limited complexity.* - *Advanced attackers capabilities (wormhole attacks), on authentication issues, as well as cellular network (LTE) security architectures.* - *First analyses of radio resilience capabilities provided by SKG and SC when facing such attacks.* - *Possible interaction of SKG and SC and classical asymmetric and symmetric ciphering schemes (e.g. how physical-layer security approaches and classical crypto-based security mechanisms can complement each other).*
D4.4	V1: 2016-08-30	*"NETSEC upgrades of existing RATs - simulation analyses complements".* This deliverable completes D4.3 with the latest results and optimization issues of our patented Physec-based secure schemes (SKG and SC). After introducing the context, recalling terminology and main notions and concepts relevant to Physec, then recalling the attacker models the complete implementation of a Secret Key Generation scheme (SKG) based on full Channel State Information (CSI), the deliverable

		provides • entropy analysis of the communication channel, • new randomness test to evaluate the quality of secret keys, • new simulation results for LTE signals and CSI • new experimental results from dual sense measured WiFi CSI. This deliverable also provides first analyses of the security upgrades provided by SKG schemes to future generation Radio Access Technologies, in a standardization perspective. Then this deliverable • recalls the secrecy coding scheme developed by the Phylaws team • proposes a new decoding algorithm issued from PPR3 discussion with reviewers) which leads to better performance • designs also new Secrecy Codes • provides new results from LTE simulated signals and from measures under WiFi carriers. This deliverable also provides first analyses of the security upgrades provided by SC schemes to future generation Radio Access Technologies, still in a standardization perspective.
D4.5	V2: 2016-10-17	*"New RATs and waveforms taking benefit of Physec upgrades – interim report".* This deliverable includes the resilience analyses and the security analyses of our patented Physec-based secure schemes when facing nominal threats. After recalling some basics for a better understanding of the content of our innovative security schemes plus the available elements of feasibility proof, it defines nominal threats (both passive and active). Then it presents the results of the resilience analyses of the security schemes, including - Radio considerations; resilience analysis, proposals for optimized implementation of the SKG SC and SP schemes into existing and future RATs. - Security analyses; crypto analyses, elements towards a security proof of the SKG and SC schemes. Enhancement proposals of the SC scheme are proposed in order to provide authentication and integrity control in addition to secrecy of messages.
D4.6	V2: 2016-11-18	*"New RATs and waveforms taking benefit of Physec upgrades – Final report".* This deliverable completes D4.5 in two senses: - First, D4.6 performs the resilience analyses and the security analyses of our patented Physec-based secure schemes when facing ultimate threats. After defining ultimate threats (both passive Huygens Fresnel Green Attack and active light–speed WormHole Attack), it presents the limits of the security schemes based on physical layer security, and several tracks to recover some resilience with the help of crypto techniques. - Then, D4.6 synthetizes the resilience analyses led over WP4 when facing both nominal and ultimate attackers, proposes and analyses optimal combinations of secure schemes that were highlighted during WP4 studies. Finally, D4.6 concludes WP4 by providing a synthesis of the technical content of our standardization proposals.

Figure 15: Deliverables of WP4

At the end of the project, WP4 has provided very complete results on all our developed and patented secured schemes, with optimization issues, convincing feasibility proof, exploration of practical performance and limits, deep resilience and security analyses when facing any kind of threats and scenarios. Thus, despite some difficulties (see above), WP4 lead and achievements were thus perfectly in line with the goals and needs of the PHYLAWS project and with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2].

Moreover,

- When considering algorithm development, task T4.2 (D4.3 and D4.4) largely overtook the initial work planned, by providing not only algorithm but also validation capabilities into WP5 and WP6.
- When considering resilience and security analyses, task T4.3 (D4.5 and D4.6) largely overtook the initial work planned, in order to compensate the late availability of massive dual sense CSI measurement output by WP5 experiments.

All over the Phylaws project, the added effort for all this added work is roughly 6 added MM.

3.2.7.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.4_PPR4slides] part E.

3.2.8- Technical Work Package 5 – Experimental study cases in 2.4 and 5 GHz Band – Extraction and application of CIRs – Development of the WiFi test bed.

3.2.8.1- Overview

WP5 Leader: CEL - Start: Month 10 - End: Month 46 - deliverable list recalled in annex 2.

This work package was initiated during period 1. Its core activity concerns mainly the end of period 2 and 3. The work of WP5 achieved during period 3 was late when compared to the revised description of work of the Phylaws project [PHYLAWS_GA-DOW2] and to the relevant planning. As a consequence:

- It was needed to change the initial experimental plan:
  - In fact, the development of the firmware met numerous difficulties especially concerning the Tx/Rx wide band calibration process under automatic gain control processing.
  - Experiments initially planned with the interceptor part of the test bed developed by partner TCS were no more possible because of time restriction.
  - Thus Eve modelling into the experiments was achieved with a third party based on CEL device, such as Alice and Bob, or with Wifi interceptors and analysers (wireshark) on PC devices.
  - On the other hand, the security analysis in WP4 was enhanced by including entropy and mutual information estimations from the CSI measurements performed at Alice Bob and Eve with the wifi test bed, as soon as they were available.
  - First version of D5.1 [PHYLAWS_D5.1] and D5.2 [PHYLAWS_D5.1] were published during March 2016, D5.1 and D5.2 were completed in April 2014
  - While a draft version deliverable D5.3 [PHYLAWS_D5.3] was published in March 2016 (M 41), its final version was published on December 2016 after the official end of the project (> M 48).
  - Deliverables D5.4 [PHYLAWS_D5.4] and D5.5 [PHYLAWS_D5.35] were published on December 2016, after the official end of the project (> M 48).

The current status of this work package during period 3 is the following:

- The TCS's hardware and firmware part of the test bed was achieved at the end of period 2. This part of test bed was intensively re-used to input WP3, WP4 and WP6 with real field records for
  - Measurements
  - Radio-channel extraction
  - Analyses of space correlation and time correlation

- Input of LTE simulation with extracted real field radio-channel as complement of the radio channel modelling
- SKG processing from extracted single sense CIR
- SC processing from extracted single sense CIR
- Sustaining dissemination and standardization initiatives with experimental data.

- The CEL's part of the test bed has achieved major progresses during starting period 3, by providing first dual sense CSI in 5 GHz Wifi carriers in December 2015.

- Nevertheless, long duration dual sense CSI at 5 GHz and 2.4 GHz carriers were available only at the ultimate end of the project (October 2016) and exploited since this date.

More details on these difficulties and their management are given in section § 3.3.9 "risk analysis".

Nevertheless, at the end of the project, WP5 succeeded to provide enough experimental material for:

- The experimental feasibility proof of all our developed and patented secured schemes,
- Optimization analyses
- Exploration of practical performance and of limits,
- Dissemination
- Standardization initiatives.

WP5's outputs also confirmed the prior conclusion of our resilience and security analyses.

Moreover, the experimental material allowed the elaboration of very complete demonstration and paper that were presented into the final work shop of the Phylaws project (PIMRC' 2016 Valencia Spain), as well as the building of journal papers and chapter books mentioned above. It also provided convincing arguments for standardization proposals.

At the end of the project, we can thus consider that despite the unexpected delays of WP5 and the relevant troubles on project management WP3 and WP4, WP5 achieved its goals and the expectations of the Grant Agreement [PHYLAWS_GA-DOW2].

The table hereafter summarizes the content of WP5 deliverables.

3.2.8.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.5_PPR4slides] part D.

Deliverable	Date	*"Title"* Summary of the content
D5.1	*Initial V1.0:* *2016-03-20* *Released V1.1* *2016-04-22*	*"WiFi test bed setup development report".* *This deliverable describes the WiFi Tesbed setup that will be used for all WP5 experiments. This document provides all information about the initial architecture of the test bed:* - *Legitimate part built, with the Wifi chipsets of Celeno, by partner Celeno.* - *Interceptor/Attacker part built with Ettus URSP devices by partner TCS.* *Moreover, D5.1 explicates how the test bed can be used for extracting dual sense CSI in Wifi bands, modeling several legitimate and attacker configurations and test countermeasures and security schemes such as* - *Artificial Noise and Beam-Forming* - *Secret Key Generation* - *Secrecy coding under radio advantage*
D5.2	*V1: 2016-03-20* *V2: 2016-04-22*	*"Experiment campaign plan".* *This deliverable includes all information about the initial experimental plan of the test bed and demonstrates the capabilities of the WiFi test bed before experimentations.*
D5.3	Draft V1: 2016-03-20 Completed V2: 2016-12-10	*"Intermediate Report on WiFi interceptor experiments with the test bed".* The draft deliverable included the first description items of experiments and storage of records performed during the experiment campaign, and it highlighted the outputs of the test beds. The completed version includes the complete description of experiments and results dedicated to Secret Key Generation under Wifi Links.
D5.4	Completed V1: Published 14 December 2016	*"Final Report on WiFi interceptor experiments with the test bed".* The completed version includes the complete description of experiments and results dedicated to Artificial Noise and Secrecy Coding under Wifi Links.
D5.5	Completed V1: To be published December 2016	*"Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades".* The completed version will be described here after its publication (In the V2 version of the present deliverable D1.5).

Figure 16: Deliverables of WP5

3.2.9- Technical Work Package 6 – Simulation study case – LTE Systems

WP6 Leader: VTT - Start: Month 12 - End: Month 46 - deliverable list recalled in annex 2.

3.2.9.1- Overview

This work package has been initiated during period 1. Its core activity concerns mainly period 2 and period 3.

The work of WP6 achieved during period 3 was perfectly in time with the revised description of work of the Phylaws project [PHYLAWS_GA-DOW2] and with the relevant planning:

- *Deliverable D6.1 was achieved on time during period 2. Nevertheless, following the recommendations of the reviewers during PPR2, a new version V.2.0. of Deliverable D6.1 was achieved (which describes*

in its appendix 8 the reasons for the choice of the MATLAB channel model from QuaDRiGa for the study of the simulator, the selected SKG and SC algorithms for further simulation plan).

- Deliverable D6.2 was delivered in May 2016.
- Deliverable D6.3, including all results of WP6, was delivered in September 2016.

The table hereafter summarizes their content.

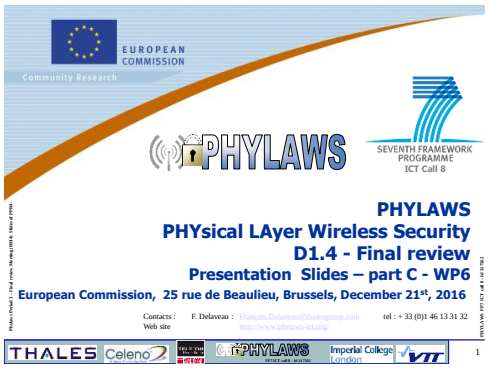
WP6 lead and achievements are perfectly in line with the goals and needs of the PHYLAWS project and with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2]. Moreover, the simulation material allowed the building of a very complete paper presented during the final work shop of the Phylaws project (PIMRC' 2016 Valencia Spain), as well as the building of journal papers and chapter books mentioned above. It also provided convincing arguments for standardization proposals.

Deliverable	Date	*"Title"* Summary of the content
D6.1	*Initial (end of period 2)* *V1: 2015-06-30* *Rev. (period 3)* *V2: 2016-02-20*	*"Modelling of LTE-based cellular system".* *See [PHYLAWS_D.1.3] for the main content description. The new version V2 details* - *the motivation for radio-channel models (QuaDRiGa versus Winer II)* - *simulation plan for SKG* - *Simulation plan for SC*
D6.2	V1: 2016-05-12	*"Simulation of interception of waveform signals in LTE-based cellular system"* This deliverable includes - A recall of the most important parts of the LTE link level simulators. - A complete description of the algorithms, simulator block diagrams and parameters, figures-of-merit, scenarios and test cases for the LTE link level performance of the LTE waveform signals with and without underlying Tag Signals. Complete results and detailed analyses are also provided. - A complete description of the algorithms, simulator block diagrams and parameters, figures-of-merit and first scenarios and test cases for the LTE link level performance of the LTE waveform signals enabling Secret Key Generation. First results and analyses are also provided. - A complete description of the algorithms, simulator's block diagrams and parameters, figures-of-merit and first scenarios and test cases for the LTE link level performance of the LTE waveform signals enabling AN-BF and Secrecy Coding. First results and analyses are also provided.
D6.3	V1: 2016-09-30	*"*LTE-based cellular system simulations - Concluding report including simulation results and proposals for standardization*"* Focusing on LTE-based cellular networks, this deliverable describes all implementations, test, performance simulations of the proposed physical-layer security schemes (Secure Pairing with Tag Signals, Secret Key Generation, Secrecy Coding), compared to the performance of a conventional transmission - Recall and complements on the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit and results for the Tag Signals Physec technique. - Recall of the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit of the Secret Key Generation PHYSEC technique. Complete results and detailed analyses. - Recall of the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit of the Artificial Noise Beam Forming and Secrecy Coding Physec techniques. Complete results and detailed analyses. - Conclusions of the simulations results and proposal for standardization.

Figure 17: Deliverables of WP6

3.2.9.2- Detail for the period3

See the presentation slides [PHYLAWS_D.1.4_PPR4slides] part C.



3.3- Project management, dissemination and standardization during the period

WP1 Leader: TCS - Start: Month 1 - End: Month 48

Work package 1 “management, dissemination, standardization, and advisory board” focuses:

- On project management (including risks issues, late deliverables, etc.).
- On project impact and visibility and on project outputs:
  - large dissemination through publications and conferences,
  - standardization proposals for improving existing radio communication systems.

It included four tasks:

- WP1.1: Overall management (leader TCS).
- WP1.2: Dissemination (leader TPT).
- WP1.3: Standardization (leader TCS).
- WP1.4: Advisory Board (leader TCS).

3.3.1- Significant results of the management activities (WP.1.1 T1.1. – D1.4&D1.5 - lead TCS)

3.3.1.1- Achievements during the period

Overall managements issues, work and achievement are detailed in § 2.3 – H and 3.2.1 above.
Recalls on dissemination activities are given in § 3.3.2.
Recalls on standardization activities are given in § 3.3.3.
Recalls on advisory board activities are given in § 3.3.4.
More details regarding the web site and its regular upgrades are given in § 3.3.5.
More details regarding networking in the consortium are given in § 3.3.6.
More details regarding management of IPRs in the consortium are given in § 3.3.7.
More details regarding management of changes in the consortium are given in § 3.3.8.
More details regarding management of risks are given in § 3.3.9.
More details regarding management of risks are given in § 3.3.9.
More details regarding management of ethical issues relevant of privacy are given in § 3.3.10

3.3.1.2- Coming back on overall management issues during the whole Phylaws project

The Phylaws project encountered numerous management difficulties:

- Due to material and staff lacks (TCS partner) during period 1.
- Due to inappropriate comportment and requirement of the first team of reviewers during PPR1/RM1, which involved serious misunderstood and confusion relevant to the project's goals and means.
- Due to redaction of a new DoW after PPR1 (on request of EC) and one year delay (on request of TCS) with suitable modifications of the reviewers' team and enhancement of consortium's staff.
- Due to development latencies of the wifi test bed during end of period 2 and start of period 3, which disturbed achievement delays of T3.4 and T3.4 into WP3, delayed into WP5 the development of the test bed (task T5.1 and T5.2) then the production of experimental results and deliverables into task T5.3, force to adapt the experimental plan of WP5 and the leading of the algorithm development and security analyses into WP4 tasks T4.2 and T4.3.

Despite these numerous management difficulties, the project management and coordination achieved the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and is line with the objectives and needs of the project.

Nevertheless these unexpected difficulties involved significant added efforts and costs to partner/coordinator TCS, and for some of the partners:

- At the end of the Phylaws project, these added efforts and costs are estimated to roughly 20 MM added effort and 326 kE added costs for partner TCS (see § 3.5 table 3.5.8: roughly 10 MM added for management leading thus to ~200 kE added costs, roughly 10 MM RTD leading thus to ~126 kE added costs).
- Note that this added effort and cost of coordinator TCS are free of charge for EC (see [PHYLAWS_D.1.2_PPR1] § 3.4 table 3.4.1, see [PHYLAWS_D.1.3_PPR3] § 3.5 table 3.5.1 and see in the present document § 3.6 table 3.6.1).

3.3.1.3- Added management work since the PPR4 review for ending the Phylaws project

Finalization of PPR4/RM4 planned 21 December 2016 Brussels.

Achievement of cost issues: audits, NEF completion.

Writing of (the present) PPR4 deliverable D1.4 released version after RM4 V2 (initially planned January 2017, delivered Marche 2017 after the return of EC [PHYLAWS_GA-CR_OL4]), including:

- Completed costs issues.
- Answer to remarks and recommendations of reviewers during RM4 and into their Consolidated Report of the final review [PHYLAWS_GA-CR_PPR4.

Upgrade of some parts of deliverables of period 3, then publishing of new versions.

Writing of the project synthesis (deliverable D1.5), planned after RM4/PPR4, initially delivered in February 2017, also updated in March 2017.

3.3.2- Significant results of dissemination activities (WP1 T.1.2, D1.8 - lead TPT)

3.3.2.1- Achievements during the period

Numerous papers and presentations of the Phylaws team occurred during the period3 - see § 2.3 - E for a synthesis and deliverable D1.8 [PHYLAWS_D1.8] for complete information. Deliverable D1.8 [PHYLAWS_D1.8], published at the end of period 3, concludes the task T1.2 of WP1.

3.3.1.2- Coming back on overall dissemination issues during the whole Phylaws project

Dissemination efforts were very intensive and fruitful during the complete project duration.

Concluded with two journal papers and two book chapters (submitted, with publication occurring year 2017), and with a very successful workshop hosted by PIMRC'2016 Valencia Spain, Sunday 4th September 2016, dissemination is one of the main success of the Phylaws project.

Dissemination actions largely overtook the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and perfectly achieved the objectives and needs of the project.

3.3.1.3- Remaining dissemination work after ending the Phylaws project

Follow and conclude the publication of our (concluding) two journal papers and two book chapters.

In the months following the end of the project, prepare

- A synthesis paper about the Phylaws' results centred on our resilience and security analyses, in line with the synthesis report ([PHYLAWS_D.1.5]).
- A paper on limitations of Physec when facing ultimate threats (in line with deliverable D4.6 [PHYLAWS_D.4.6]).

3.3.3- Significant results of standardization activities (WP1 T.1.3, D1.11 – lead TCS)

3.3.3.1- Achievements during the period

Numerous participations and contributions of the Phylaws team occurred during the period - see § 2.3 - F for a synthesis and Deliverable D1.11 [PHYLAWS_D1.11] for detailed information. Deliverable D1.11 [PHYLAWS_D1.11], published at the end of period 3, concludes the task T1.3 of WP1.

3.3.3.2- Coming back on overall standardization issues during the whole Phylaws project

Despite the inherent politically/diplomatically difficulties of standardization actions, our efforts were fructuous at the end of the period 3:

- Several of our contribution proposals were accepted at 3GPP SA#3 and ITU WP 5G.
- At the end of the project, Phylaws deeply disseminated among stakeholders and regulators, and impacted standardization bodies such as 3GPP and ITU-R.

Finally, our standardization initiatives and results should be considered as a success of the Phylaws project, and Standardization actions perfectly match the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and achieved the objectives and needs of the project.

3.3.3.3- Remaining standardization after ending the Phylaws project

Participate and contribute to some of the next 3GPP SA3 meeting in order to concretize our last proposal relevant to Secured Paring with Tag Signals.

Redact parts of 3GPP documents relevant to the usage of "3GPP-agreed" security/Physec contributions of Phylaws for security into next generation RATs.

Participate and contribute to the newt ITU WG 5D meetings, in order to concretize our last proposal relevant to ITU-R reports.

3.3.4- Significant results of Advisory Board activities (WP.1 T1.4, D1.13 and D1.14 – lead TCS)

3.3.4.1- Achievements during the period

The second Advisory Board meeting occurred in the middle of period3, the relevant report is the deliverable D1.13 [PHYLAWS_D1.13]. The deliverable D1.14 [PHYLAWS_D1.14], published at the end of period 3 concludes the task T1.4 of WP1 with a synthesis of AB activities requirements and a detailed explanation of the consequent actions led by the Phylaws consortium.

3.3.3.2- Coming back on overall Advisory Board issues during the whole Phylaws project

Advisory Board actions were very fruitful for the Phylaws project, not only on standardization activities but also on technical development and dissemination strategy.

Despite the cancelling of the third Advisory Board meeting (see explanation synthesis into § 2.3 – G and justifications in deliverable D1.14), Advisory Board actions are perfectly in line with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and with the objectives and needs of the project.

3.3.5- Upgrade of the project website

Public site: See: http://www.phylaws-ict.org.

Partners's dedicated site: See
https://e-ecm.online.corp.thales/livelink/livelink.exe/open/tcsehatphylaws/?name=_TCS__e_HAT_Phylaws

EC's dedicated site: See
https://e-ecm.online.corp.thales/livelink/livelink.exe?func=ll&objId=1184473&objAction=browse&sort=name.

The Upgrade of the project web site was continuous during period 3. Moreover, it will continue after the end the project. The upgrades of period 3 took into account the recommendations of the reviewers during the last PPR2:

- All papers and presentation (except presentation at EDA Captech 31 which involves some military considerations) were published by the consortium (including PhD thesis), in pre-publication format or in final published format, at the public web site.
- All technical deliverables (WP2 to WP6) are published in Pdf format at the public web site, also at the EC reserved part of the web site.
- All dissemination deliverables (WP1 T1.2) are published in Pdf format at the public web site, also at the EC reserved part of the web site.
- All standardization deliverables (WP1 T1.3) are published in Pdf format at the public web site 3), also at the EC reserved part of the web site.
- All Advisory Board deliverables (WP1 T1.4) are published in Pdf format at the public web site, also at the EC reserved part of the web site.
- All management deliverables and relevant exchanges with EC and reviewers (outcome letters and consolidated reports etc.) are published at the EC reserved part of the Phylaws web site).

In addition, note that all deliverables uploaded at the EC part of the Phylaws web site are now High Resolution pdf format.

The project web site is perfectly in line with the expectations of the Grant Agreement [PHYLAWS_GA-DOW2] and with the objectives and needs of the project.

3.3.6- Networking – Discussion with other funded projects (lead TCS)

3.3.6.1- Achievements during the period

See § 2.3 – H2

3.3.6.2- Coming back on overall discussion issues during the whole Phylaws project

Our contacts with projects such as Duplo and Prophylaxe were very fruitful for the technical achievement and direction of our study and development tasks.

Our contacts with project 5G-Ensure and Prophylaxe were also fruitful regarding synergies and mutual support at standardization bodies (especially at ETSI, at 3GPP and at ITU-R 5G).

3.3.6.3- Discussion work after ending the Phylaws project

As 5G-Ensure started end 2015 and deals with 5G Security, Phylaws provided inputs relevant to threats at Physical Layer, and solutions derived from proven Physec concepts.

On the counterpart, it is expected that 5G-Ensure will continue to provide economic scenarios about 5G Security, and long term perspectives for the "carrier" continuation of Phylaws' solutions into 5G standards, as part of a global security solution for 5G networks.

Share of standardization issues will thus continue with projects 5G-Ensure towards 3GPP and ITU.

3.3.7- IPR strategy (lead TCS)

3.3.7.1- Work done during the project

Three patents were written in French language to be submitted to French patent office in December 2015:

- The first one focuses on Secure Pairing [PHYLAWS_Patent1].
- The second one focuses on Secret Key Generation [PHYLAWS_Patent2].
- The third one focuses on Secrecy Coding under radio advantage of Bob to Eve [PHYLAWS_Patent3].

The current status of these three patents is the following:

- Publicity was authorized from March 2016.
- Agreement by the French patent office was achieved end 2016. The official granting should occur at the end of 2017.
- International extensions and IPR issues are under examination by the legal entities of each partner, from an initial IPR repartition and cost evaluation submitted by TCS.

Regarding IPR issues at the end of the Phylaws project, TCS alone, as coordinator, paid for the French redaction and deposit of patents; IPR repartition among partners is proposed by TCS; Europe and Word extension policies are examined; costs relevant to patent translation and deposit are estimated.

The official references of the existing deposit (French patent bureau for now) are the following:

Invention 1 : "secure pairing"

No. de dépôt :	1502713
Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE D'ASSOCIATION UNIVALENTE ET UNIVOQUE ENTRE EMETTEURS ET RECEPTEURS DE TRANSMISSION A PARTIR DU CANAL DE PROPAGATION
Inventeurs :	François DELAVEAU, Renaud MOLIERE, Christiane KAMENI NGASSA, Claude LEMENAGER, Adrian KOTELBA, Jani SUOMALAINEN
Déposants:	THALES, TEKNOLOGIAN TUTKIMUSKESKUS VTT

Invention 2 : "secret key generation"

No. de dépôt :	1502712

Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE D'EXTRACTION UNIVALENTE ET UNIVOQUE DE CLES A PARTIR DU CANAL DE PROPAGATION
Inventeurs :	Renaud MOLIERE, Christiane KAMENI NGASSA, François DELAVEAU, Claude LEMENAGER, Alain SIBILLE, Taghrid MAZLOUM, Nir SHAPIRA
Déposants :	THALES, TELECOM ParisTech, CELENO COMMUNICATION LTD

Invention 3: “secrecy coding”

No. de dépôt :	1502710
Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE DE CODAGE UNIVOQUE ET SECRET DE TRANSMISSION SUR UN CANAL DE PROPAGATION A AVANTAGE DE CAPACITE
Inventeurs :	Christiane KAMENI NGASSA, François DELAVEAU, Jean-Claude BELFIORE, Cong LING
Déposants :	THALES, TELECOM PARIS TECH, IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

Note1: The potential use by industrial partners is clear when reading the patent content:

- The first one relies to better pairing of terminals and nodes for authenticated radio links negotiations
- The second one relies to better protections of signalling and access messages in any TDD RAT thanks to SKG schemes
- The third one relies to better protections of signalling and access messages in any RAT thanks to SC schemes

Note2: The patents’ description are on the partner private part of the Phylaws web site. They will be published at the Phylaws public web site (French language) after official acceptation by the French patent bureau.

3.3.7.2- Work on IPR after ending the Phylaws project

Extend the patents to Europe US and Canada, Asia etc. after official granting by the French patent bureau. At the end of the Phylaws project The PCT (“*Patent* Cooperation Treaty”) process is already in progress for the three patents mentioned above.

Share IPRs and costs among partners. Achieve the exploitation plan of the patents.

Figure 18 below completes the information above by providing detail about inventors and IPR + Costs share proposal.

3.3.8- Change in the consortium - Changes into legal status of any of the beneficiaries (VTT)

Partner VTT asked for change of his budget allocation relevant to travel and accommodations - see Figure 19 below. This request was accepted by EC during period 3, and costs’ reporting above into § 3.5 takes into account this changes.

Other partners: Nobody else asked for changing budget allocation.

PHYLAWS PATENTS - INVENTOR AND INTELLECTUAL PROPERTY					
			PATENT PROPOSAL		
			n°1	n°2	n°3
			Key-free security of AIR interface in wireless communications by using radio propagation random for secure pairing of electonic devices	Key-free security of AIR interface in wireless communications by using radio propagation random for generating secret keys	Key-free security of AIR interface in wireless communications by using radio propagation random for enabling secret codes
CURRENT STATUS					
TCS REFERENCE			TCSINV15_517	TCSINV15_518	TCSINV15_519
CABINET REFERENCE			070151 FR	070152 FR	070153 FR
PATENT NUMBER			**Date 29/12/2015 Number 1502713**	**Date 29/12/2015 Number 1502712**	**Date 29/12/2015 Number 1502710**
	CEE EXTENSION		TBD after delivery of french patent	TBD after delivery of french patent	TBD after delivery of french patent
	PST		TBD after delivery of french patent	TBD after delivery of french patent	TBD after delivery of french patent
	GCC		TBD after delivery of french patent	TBD after delivery of french patent	TBD after delivery of french patent
	others		TBD after delivery of french patent	TBD after delivery of french patent	TBD after delivery of french patent
Inventor proposal					
	F. Delaveau	TCS	xx	x	x
	C. Kameni	TCS	x	x	xx
	R. Molière	TCS	x	xx	
	C. Leménager	TCS	x	x	
	A. Sibille	TPT		x	
	T. Mazloum	TPT		x	
	J.C. Belfiore	TPT			x
	C. Ling	ICL			x
	A Kotelba	VTT	x		
	J. Suomalainen	VTT	x		
	N Shapira	CEL		x	
IPR proposal			**n°1**	**n°2**	**n°3**
	TCS		**80%**	**60%**	**60%**
	TPT		**0%**	**30%**	**30%**
	ICL		**0%**	**0%**	**10%**
	VTT		**20%**	**0%**	**0%**
	CEL		**0%**	**10%**	**0%**
	Total		**100%**	**100%**	**100%**
Cost indication (hyp: TCS assumes the redaction, patent costs are shared under IPR percentage					
			n°1	**n°2**	**n°3**
	Year 2015		8 kE	6.5 kE	6.5 kE
	Year 2016		1.5 kE	1.5 kE	1.5 kE
	Year 2016		35 kE	35 kE	35 kE
	2016-2020		12 kE	12 kE	12 kE
	after 2021		?	?	?

Figure 18: Patents of Phylaws – Inventor and IPR status

PHYLAWS VTT								
Old budget								
	RTD/Innovation activities	**Demonstration activities**	**Training activities**	**Coordination**	**Support**	**Management activities**	**Other**	**TOTAL**
Personnel costs	316 431	0	0	0	0	6 246	0	322 677
Subcontracting	0	0	0	0	0	1 500	0	1 500
Other direct costs	65 000	0	0	0	0	0	0	65 000
Indirect costs (incl.Res.Facility Costs)	272 131	0	0	0	0	5 371	0	277 502
Lump sum, flat rate or scale of unit (option	0	0	0	0	0	0	0	0
Total budget	653 562	0	0	0	0	13 117	0	666 679
Requested EC contribution	490 172	0	0	0	0	13 117	0	503 289
Total receipts								0
New budget								
	RTD/Innovation activities	**Demonstration activities**	**Training activities**	**Coordination**	**Support**	**Management activities**	**Other**	**TOTAL**
Personnel costs	338 053	0	0	0	0	6 246	0	344 299
Subcontracting	0	0	0	0	0	1 500	0	1 500
Other direct costs	25 000	0	0	0	0	0	0	25 000
Indirect costs (incl.Res.Facility Costs)	290 509	0	0	0	0	5 371	0	295 880
Lump sum, flat rate or scale of unit (option	0	0	0	0	0	0	0	0
								0
Total budget	653 562	0	0	0	0	13 117	0	666 679
Requested EC contribution	490 172	0	0	0	0	13 117	0	503 289
Total receipts								0

Figure 19: Budget re-allocation – partner VTT

3.3.9- Risk analysis and risk Management (lead TCS)

3.3.9.1. Late delays of firmware achievement into the CEL test bed WP5 - impact on other WPs

Origin of the risk: difficulty and latency on the firmware development of the Wifi test bed.

For technical explanations about this risk, see [PHYLAWS_D.1.3_PPR3slides] part F and [PHYLAWS_D.1.3_PPR3], that accurately describe the test bed development and the difficulties met by partner CEL during period 3 of the project.

The consequences of the late development of the Wifi test bed at WP3 channel experiments were:

- "Roughly" calibrated dual sense CSI records in the 5 GHz and 2.4 GHz were available with the wifi test bed only by June 2016. Moreover the time duration of the record was very short (only a few snapshots).
- Calibrated dual sense CSI records in the 5 GHz and 2.4 GHz over significant time duration measured by the wifi test bed were only available at the end of October 2016 (M48).

As D3.4 and D3.5 were dependent on these CSI recording, the consequences were:

- Significant increased delay for achieving the completed version V2 of deliverable D3.4 [PHYLAWS_D3.4], published on November 2016 (M49), while only a partial version V1 was published on March 2016 (M41).
- Added delay for deliverable D3.5 [PHYLAWS_D3.5], firstly postponed to September 2016 (M47), and finally published at the beginning of December 2016 (M50).

Corrective actions:

The corrective actions were mainly the intensive redaction activity of partners TCS and CEL during the M47-M49 period in order to overcome the increased delay for available experimental data.

Nevertheless, it is noticeable that at the end of the Phylaws project:

- There is no lack of experimental data on the radio channel.
- The content of deliverable D3.4 [PHYLAWS_D3.4] and D3.5 [PHYLAWS_D3.5] remain very accurate and full of interesting new results. In addition, the results of [PHYLAWS_D3.4] and [PHYLAWS_D3.5] confirm enhancements and accurate results achieved in WP4 with long time duration records available at the end of the project. The experimental prof enhancement are relevant to:
  - channel randomness properties.
  - TS, SKG and AN-BF+SC feasibility proof and performances.

Finally, the test bed development delay had no impact on the content of WP3, only on its achievement delay.

The consequences of the late development of the Wifi test bed at WP5 experiments were the following:

No more time was left from August 2016 (M46) to October 2016 (M48) for performing interception experiments and development of radio attacks of the secure schemes implanted under Wifi links (that needed reliable dual sense transmission between Alice and Bob over long time duration and numerous recording instances). The project ended year October 2016, 6 months at least were necessary for these interception experiments and relevant attack developments while after July 2016, it was clear that no massive (well-calibrated) CSI records would be available before September 2016. Also it was no ore possible to lead attack experiments and developments.

The consequences of the late development of the Wifi test bed at WP5 deliverables were the following:

- Added delay for the final version of deliverable D5.3 [PHYLAWS_D5.3] (preliminary draft delivered March 2016, final version initially postponed August 2016 (M46), finally published on December 2016 (Month 50)), while first CSI records needed for experimental channel study and SKG attempts at 2.4 GHz wifi carrier were available since mid-June 2016 only and correctly calibrated CSI sample over long time duration available at 5 GHz and 2.4 GHz carrier in September 2016 only.
- Added delay for the final version of deliverable D5.4 [PHYLAWS_D5.4] (same reason as above), finally planned December 2016 (Month 50).
- Added delay for the final version of deliverable D5.5 [PHYLAWS_D5.5] (same reason as above), finally planned December 2016 (Month 50).

Corrective actions:

The redaction of draft of partial version of deliverables D5.1 [PHYLAWS_D5.1], D5.2 [PHYLAWS_D5.2] and D5.3 [PHYLAWS_D5.3] started as soon as possible, then completed with completed experimental data.

WP4 significantly supported the development and the validation of the wifi test bed into WP5.

The consequences of the late development of the Wifi test bed at WP4 studies were the following:

First, as no interception experiment with the TCS's interceptor and the CEL's Wifi test bed could be achieved before Month M46 because of the lack of time at the end of period 3, partner TCS had to deeply modify the initial approach for the resilience and security analyses, especially in deliverables D4.5 [PHYLAWS_D4.5] and D4.6 [PHYLAWS_D4.6].

Second, as only "few" calibrated dual sense CSI records over very short time duration were available until end of Month 47, only a few channel snapshots were available to perform the security analysis. The estimation accuracies of entropy and mutual information performed into WP4 security analyses were thus initially quite rough into deliverable D4.5 [PHYLAWS_D4.5].

The security analyses had to take into account the available recorded material and to process in a different way than initially planned:

- First, in the early stages of the security analysis, we used the available long-time duration (single sense) CIR records performed during period 2 and starting period 3 with the TCS interceptor part of the test bed were intensively re-exploited for security analyses (in addition to channel analysis into WP3). This allowed to study and assess:
  - Channel diversity issues and impacts on key privacy (SKG) and index privacy (SP).
  - Tuning of SKG and SC parameters.
  - Feasibility assessment and prior performance estimation of SKG and SC schemes.

- Then short time duration dual sense CSI records provided by the Wifi test bed at the second half of the period 3, e.g. from May to September 2016 (M43-M47) were exploited with several instances of the Wifi test bed modelling Alice Bob and Eve, all operated by partner CEL (instead of having Eve operated by the TCS interceptor). The security analyses had to process with min-entropy and bounds of mutual information at legitimate and attacker side

- During the second half of the period 3, e.g. from May to September 2016 (M43-M47), the few available short time CSI dual sense snapshots were also used in order:
  - To study reconciliation issues, and tune the channel de-correlation pre-processing, the quantization and the correction coding into SKG.
  - To achieve first (and rough) estimations of min–entropy and min mutual information of the channel at legitimate and attacker side, which provided lower bound of secrecy and privacy capabilities of the Physec-based schemes.

- Finally, longer time duration CSI records being available since August 2016 (M46), still with several instances of the Wifi test bed modelling Alice Bob and Eve, allowed more accurate estimations of entropy and mutual information of the channel at legitimate and attacker side, that confirmed and enhanced the previous results of the security analysis into WP4. Relevant results are given in detail into deliverable D3.5 [PHYLAWS_D3.5]

The consequences of the late development of the Wifi test bed at WP4 deliverables were the following:

Significant added TCS efforts were required to mitigate risks of wifi test bed WP5, to help CEL with analysis of SKG and SC results from the test bed records, radio and algorithm expertise for development validation and deliverable redaction, search for optimal tuning of SKG and SC algorithms. The redaction of deliverables D4.5 [PHYLAWS_D4.5] and D4.6 [PHYLAWS_D4.5] was thus postponed to M47-48.

The management of the security analysis into WP4 had also to take into account the new constraints induced by WP5 late delays and data record limitations.

Corrective actions:

The redaction of deliverables D4.5 [PHYLAWS_D4.5] and D4.6 [PHYLAWS_D4.8] started as soon as recorded data was available. This was later than initially planned, but early enough to point out:

- the main security trends of Physec-based schemes when facing nominal threats [PHYLAWS_D4.5], then confirmed and precised by our latest (long time duration) records and analyses into D3.5 [PHYLAWS_D3.5]
- the main security trends of Physec-based schemes when facing ultimate threats [PHYLAWS_D4.6],

and elaborate a synthesis of security issues [PHYLAWS_D4.6].

Finally, it is noticeable that even if WP4 was somehow disturbed by the late delays of experimental data,

- there is no lack in the security analysis: all aspects have been covered (privacy, confidentiality, authentication, etc…),
- several kind of threats have been taken into account (nominal and ultimate, passive, active including MITM)
- the content of deliverable D4.5 and D4.6 remain very accurate and full of interesting results and proposals for standardization.

Finally, the test bed development delay had no impact on the content of WP4, but only on the management and the achievement delay of the security analyses.

3.3.9.2- Risks due to added charge relevant to report redaction (WP1 task T1.1):

Origin of the risk:

Since the acceptation of the new DoW [PHYLAWS_GA-DOW2], the management activities included many added redaction efforts: intermediate review and associated report (1 MM work), 3 QMRs till the end of the project, etc.

Most of the information spread over the management is quite redundant, while the redaction time and effort remain significant and the project teams and costs are limited.

The consequences of the increasing management redaction tasks were the following:

The time spent for added management report redaction reduced the study effort on the most advanced Physec concepts. For example, because of all the added redaction work, it appeared at the second half of

period 3 that no enough time and personal budget for the TCS team would be left for achieving a complete experimental proof of SP with TS and IAS.

Corrective actions:

- We reduced the redaction work by referencing as most as possible the redundant information over periods.
- We limited the number of QMRs to 2, the last sub-period M45-M48 being covered by the present deliverable D1.5.
- We limited the size and content of the QMRs.
- We limited the time and expenditures relevant to Advisory Board:
  - The essential messages of the AB members were expressed during meeting 1 and 2 (January 2016) and convert into practical actions by the Phylaws team (see Deliverable D1.14 [PHYLAWS_D1.14])
  - The initial planning of the third AB meeting in PIMRC'2016 was no more possible because of duration reduction of the Phylaws Workshop to one half day instead of a full day.
  - Finally the last AB meeting was cancelled in order to better concentrate on standardization issues (concretization of our 3GPP and ITU contributions see [PHYLAWS_D.1.11]) and dissemination issues (final Work Shop hosted by PIMRC'2016 Valencia – book chapter, journal papers – see [PHYLAWS_D1.8]).

3.3.9.3- Delays risks for standardization outputs (WP1, task T1.3).

Origin of the risk:

Standardization activities and results are accurately described in deliverable D1.11 [PHYLAWS_D.1.11].

Despite the efficiency of our actions all over the Phylaws project (especially during its last period 3), there was a risk that standardization bodies (being neither scientific congresses nor technical meeting but looking closer to commercial perspectives), would accept only "minimal version" of our proposals, even after intensive efforts of Phylaws partners.

Corrective actions.

We had to "continue and insist" even after M48 on standardization efforts, that was successful only in the recent Tenerife SA3#85 meeting (November 2016).

We recall that the total benefit of our initiatives should happen next year only, thus after the end of the Phylaws project.

Finally, it is noticeable that even if task T1.3 was a difficult diplomatic job with significant "randomness" to manage inside standardization bodies, the end results of our standardization actions at 3GPP and ITU are concrete and significant.

3.3.10- Ethical issues relevant to privacy

3.3.10.1- Brief summary of the background

Privacy and citizen right issues are always associated with projects dealing with increase of communication privacy, because of policies requirements and needs, and because of security items. With regard to the legal security awareness systems and actions (such as prevention of terrorist attacks), four European norms should be considered that comprise two international treaties between the 43 Member States of the Council of Europe and two supranational rules of the European Union and its 15 Member States:

- European Human Rights Convention: Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe of 4 November 1950 (ETS. No.5)

- European Convention on the Automated Processing of Personal Data: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 28 January 1981 (ETS No.108)

- European Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and the free Movement of such Data

- Charter of Fundamental Rights of the European Union proclaimed by the European Council in Nice on 7 December 2000

European policies direct the adoption of privacy by technical standardisation, market intervention and legal norms. In particular, Article 8 of the European Human Rights Convention, the European Convention on the Automated Processing of Personal Data of the Council of Europe and the Data Protection Directive (95/46/EC) of the European Union all have an impact on polices, legal actions, and security awareness actions by private bodies. For public bodies, although prevention of terrorist attacks security awareness actions need a legal basis of need according to the Human Rights Convention, it is not affected by the European data protection provisions since its regulation remains the realm of national member legislation. Same considerations apply for awareness of privately operated systems without data storage capabilities (e.g. communication signal recording).

3.3.10.2- Discussion of the practical consequences for the PHYLAWS project - relevant corrective actions

The wide variety of privacy and data-protection legislation across Europe should impact the PHYLAWS project and the future exploitation of its innovative technological outputs.

To avoid any risk regarding privacy issues, the PHYLAWS project and especially its experimental tasks were organized in such a manner that

- No privacy leakages risks should occur for users of radio-communications networks
- No hard interaction constraints of Phylaws' security solutions with lawful and network engineering considerations should reduce the benefit of the PHYLAWS project for the EC.

Then at the end of the project and during standardization actions, the Phylaws consortium oriented the developments innovations and standardization proposals to keep as neutral as possible to network engineering of upper protocol layers, to lawful interception systems, to governmental policies and intelligence actions.

In practice, the consortium identified three types of ethical considerations related to the project experiments and to the future usages of the innovation created into the project. We answered to these considerations in the following manner described below.

3.3.10.3- Privacy and disturbance cautions relevant to experiments:

No collection of real subscriber data occured during the experiments of the project. The data collected were only:

- Broadcasted signalling channels in the 2G/3G/4G/Wifi real field networks, without any subscriber sensitive data. During channel measurements into WP3, only broadcast signals were recorded and processed, which content includes no private information. Functionally speaking, what we performed on the radio links is similar to the sensing and measurement stages implemented into terminals themselves.

- Artificial wifi user signals were simulated and transmitted and recorded over the air: No real wifi subscriber's signals (neither signalling nor data) has been intercept or analysed. During dual sense CSI records under 2.4 GHz and 5 GHz wifi carriers (into WP3 and WP5), wifi signals were generated and recorded by the test bed itself, without any interaction with other wifi terminal or Access Point in the

neighbourhood. In order to avoid confusions risks with real communication in progress in neighbor networks, the transmitted artificial signal were fully identified and controlled by carrier, signal and spectrum shape, modulations characteristics, and finally by an artificial message content which included a prior known pattern.

3.3.10.4- Neutrality of the Physec-based security improvements with respect to lawful interception, policies, legal and intelligence governmental organizations

Our studies and standardization proposal (see [PHYLAWS_D1.11] and a synthesis of the relevant technical arguments in [PHYLAWS_D4.6]) highlighted that all the Physec-based protections proposed by the Phylaws project, being dedicated to the radio interface, have no significant impact on lawful interception at the core network:

- The intrinsic Physec-based protections end as soon as messages are decoded in the node and terminal, they also do not modify higher protocol layer.
- Even at the radio link, the Physec-based protections can easily be shortcut when needed and relevant,
  - with “generated keys” forced to values ‘0…0’ or to values known by policies and intelligence organizations
  - with “generated keys” forced to restricted lengths
  - with “secret codes” limited to inner codes (e.g. existing correction codes without secrecy capabilities),
  - etc.

Note that this important results were in the minds of the Phylaws team members till the start of the project because these requirements are more or less necessary for standardization issues too: limit the impact a the physical and MAC protocol layer, don’t disturb lawful interception and governmental policies + intelligence actions.

3.3.10.5- Exploration of the Ethical impact of the project outputs for future use of the project innovation

Ethical and legislative issues concerned by the future use of the PHYLAWS outputs have been shortly explored at the end of the project, in a way that PHYLAWS is expected to strongly upgrade protection of wireless transmissions for the citizen at the radio interface.

As noted above, our innovations avoids the main “collision risk” with governmental actions on public networks, because

- our protections operate a the physical layer only risk, and can be easily shortcut if needed,
- polices, judiciary and intelligence administrations operate mainly at core network when communication interceptions are needed and relevant.

Finally, PHYLAWS (and future researches relevant to Physec) should not impact legislation, while the secrecy extracted at the physical layer is not propagated into higher level protocol layers.

Ethical issues table

The table above was prior initiated in the Description of Work of the PHYLAWS project [PHYLAWS_GA-DOW2]. It is recalled and updated below by considering the complete results of the project:

	YES	PAGE
Informed Consent		
• Does the proposal involve children?	**No**	
• Does the proposal involve patients or persons not able to give consent?		
• Does the proposal involve adult healthy volunteers?		
• Does the proposal involve Human Genetic Material?		
• Does the proposal involve Human biological samples?		
• Does the proposal involve Human data collection?		
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?	**No**	
• Does the proposal involve Human Foetal Tissue / Cells?		
• Does the proposal involve Human Embryonic Stem Cells?		
Privacy		
• Does the proposal involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)	**No**	
• Does the proposal involve tracking the location or observation of people?	**No**	
Research on Animals		
• Does the proposal involve research on animals?	**No**	
• Are those animals transgenic small laboratory animals?		
• Are those animals transgenic farm animals?		
• Are those animals cloned farm animals?		
• Are those animals non-human primates?		
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)	**No**	
• Impact on local community		
Dual Use		
• Research having direct military application	**No**	
• Research having the potential for terrorist abuse	**Avoided by a careful design of the project innovations**	
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?	**No**	
I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO THE PROJECT	**YES**	

Figure 20: Table of Ethical issues of PHYLAWS project

3.3.10- Lawful interception, policies intelligence and legal issues

See § above “Ethical issues relevant to privacy” were lawful issues of the PHYLAWS project are discussed.

3.3.11- Problems encountered and solutions

See the risk management issues above (§ 3.3.9 “risk management”). With some modifications of the technical leading and added delays for the publication of some of the deliverables, all risks were erased at the end of the project, whose content did not suffer of the risks consequences.

3.3.12- Project planning and status

Leadership and achievement of all management dissemination standardization Advisory Board tasks matched with the new DoW schedule - see above.

At the end of the project, leadership and achievement of all technical work packages match with the new planning, despites late delays that occurred in WP5 and consequences at other WP3 and WP4 - see explanations in § 3.3.9 “risk management” above.

3.3.13- Impact of the deviations from the planned milestones and deliverables

None at the content of the project’s deliverables.

None at the feasibility proof of Physec-based protections performed into WP4 WP5 WP6

Late delays occurred for some of the deliverables’ publication at the end of period 3 - see explanations in § above, and especially § 3.3.9 “risk management”.

3.4- Deliverables and milestones tables

3.4.1- Deliverables

The table below indicates the deliverables due in the reporting period. It corresponds to the Annex I to the Grant Agreement [PHYLAWS_GA-DOW2], which has been uploaded by the partners, approved and submitted by the Coordinator TCS. Note that the periodic reports and the final report, even not considered as deliverables, are mentioned in the tables below for complete information.

- When a deliverable has been cancelled or regrouped with another one, it is indicated in the column "Comments".
- When a new deliverable is proposed, it is indicated in the column "Comments".
- This table is cumulative: all deliverables from the beginning of the project are indicated.

The acronym signification of the nature of deliverables is the following:
PU = Public
PP = Restricted to other programme participants (including the Commission Services).
RE = Restricted to a group specified by the consortium (including the Commission Services).
CO = Confidential, only for members of the consortium (including the Commission Services).
EU restricted = Classified with the mention of the classification level restricted "EU Restricted"
EU confidential = Classified with the mention of the classification level confidential “EU Confidential"
EU secret = Classified with the mention of the classification level secret "EU Secret"

- When non-highlighted, the references are relevant to contracts and deliverables of period 1: Months 1 to 12.
- The yellow-highlighted references are relevant to contract’s modifications and added deliverables that were achieved during to period 2: Months 13 to 32.
- The blue-highlighted references are relevant to deliverables of period 1 that were achieved during period 2: Months 13 to 32.
- The green-highlighted references are relevant to deliverables of period 2: Months 13 to 32.
- The grey-highlighted references are relevant to deliverables of period 1 and 2 that were upgraded during period 3 after PPR2 (hold in Brussels 9 September 2015) in order to match the recommendations of the reviewers and of the EC.
- The pink-highlighted references are relevant to deliverables of period 3 published during the period Months 33 to 40.
- The pigeon blue references are relevant to deliverables of period 3 that were published since the intermediate technical review at month 41.
- The pigeon blue underlined references are relevant to deliverables of period 3 that were published after PPR4 (after Month 50).

TABLE 1. DELIVERABLES

Del. no.	Deliverable name	Version	WP	Lead beneficiary	Nature	Dissemination level[4]	Delivery date from Annex I (proj month)	Actual/ Forecast delivery date (dd/mm/yyyy)	Status	Contractual	Comments
D1.1	Kick-off meeting. ManagT Plan, risk evaluation, analysis of ethical Issues. Minutes of K.O. meeting. Draft of Consortium Agreement.	1.0	1	TCS	MngT	PP	T0+1	30/1/2013	Submitted Accepted	Yes	None
AP	Action Plan	1.0	1	TCS	MngT	PP	T0+17	25/05/2014	Submitted Accepted	No	By request of EC
DOW2	Revised DoW	2.2	1	TCS	MngT	PP	Delivered T0+26	19/12/2014 accepted by EC T0+28	Submitted Accepted	No	To answer PPR1 recommend. of reviewers and EC
D1.1 V2		2.0	1	TCS	MngT	PP	T0+31	none	Submitted Accepted	No	Upgrade of the managT plan + slides of the restart Kick-off meeting in Paris 2015, May 22
D1.2 PPR1+ slides	Year 1 status meeting and report	3	1	TCS	MngT	PP	T0+12	20/02/2014	Submitted Accepted	Yes	Initial V1.0, delivered at T0+12, was rewritten (V1.3) following PPR1 recommendations of experts & EC
D1.3	Months 13-32 PPR2 and review meeting RM2	1.0	1	TCS	MngT	PP	T0+32	30/7/2015	Submitted Accepted	Yes	none
D1.3a PPR3+ Slides	Months 32-41 intermediate technical review meeting Slide presentation	1.0	1	TCS	MngT	PP	T0+40	20/03/2016	Submitted Accepted	Yes	PPR3 : report and slide presentationof the review meeting ref [PHYLAWS_D.1.3_PPR3slides
D.1.3 qmr1	Project quarterly month report 1	1.1 2.1	1	TCS	MngT	PP	T0+40	15/03/2016 04/07/2016	Submitted Accepted	Yes	By request of EC
D.1.3 Qmr2	Project quarterly month report 2	1.0	1	TCS	MngT	PP	T0+44	08/07/2016	Submitted Accepted	Yes	By request of EC
D.1.3 Qmr3	Project quarterly month report 3	1.0	1	TCS	MngT	PP	T0+44	08/07/2016	Cancelled	Yes	Cancellation accepted by EC
D1.4	Months 33-48 PPR4 and	1.0	1	TCS	MngT	PP	T0+48	Init 10/12/2016	Submitted	Yes	PPR4 :present document

PPR4+ slides	review meeting RM4, incl ethical issues and Risk analysis							Updated V2.0 3/3/2017	Accepted		associated with presentation slide prepared for the review meeting ref [PHYLAWS_D.1.4_PPR4slides
D1.5	Project Synthesis	1.1	1	TCS	MngT	PP	T0+50	21/02/2017 Updated V1.2 3/3/2017	V1.1 Submitted Accepted	Yes	None
D1.6	Dissemination planning report	1	1	TCS	MngT	PU	T0+3	30/1/2013	Submitted Accepted	Yes	None
D1.7	Dissemination intermediate report	1.1	1	TCS	MngT	PU	T0+30	30/5/2015	Submitted Accepted	Yes	None
D1.8	Dissemination final report	1.0	1	TCS	MngT	PU	T0+48	31/10/2016	Submitted Accepted	Yes	None
D1.9	Standardization planning report	1	1	TCS	MngT	PU	T0+3	30/1/2013	Submitted Accepted	Yes	None
D.10	Standardization intermediate report	1.1	1	TCS	MngT	PU	T0+30	30/5/2015	Submitted Accepted	Yes	None
D.11	Standardization final report	1.0 1.1	1	TCS	MngT	PU	T0+48	3/11/2016 13/11/2016	Submitted Accepted	Yes	Version 1.1. includes the reporting of the Tenerife SA3#85 meeting which held first week of Nov. 2016.
D1.12	Advisory board meet report 1	1	1	TCS	MngT	PU	T0+12	8/11/2013	Submitted Accepted	Yes	Meeting minutes and presentation slides.
D1.13	Advisory board meet. report 2	1	1	TCS	MngT	PU	T0+36	12/02/2016	Submitted Accepted	Yes	Meeting minutes and presentation slides.
D1.14	Advisory board meeting Synthesis report 3	1	1	TCS	MngT	PU	T0+48	10/11/2016	Submitted Accepted	Yes	Final synthesis of AB meetings 1 and 2 and description of relevant actions by the consortium
D2.1	Analysis of the threat counter-measure and self-protection techniques in existing and new standards	1.0 2.0	2	VTT	Techn	PU	T0+8	28/6/2013 28/12/2015	Submitted Accepted Updated	Yes	Updated version V2 with most recent threats evolutions (support for standardization actions)
D2.2	Security architectures in wireless terminal	1.0	2	TCS	Techn	PU	T0+10	23/9/2013	Submitted Accepted	Yes	None
D2.3	Fundamental aspects of physical layer security	1.1	2	ICL	Techn	PU	T0+12	14/11/2013	Submitted Accepted	Yes	Initially version V1.0 Delivered month 12. Updated V1.1 version delivered Month 25
D2.4	New opportunities provided by modern wave forms and sensing/measure of radio environments	2.0 3.0	2	TCS	Techn	PU	T0+20	30/06/2014	Submitted Accepted	Yes	Initially planned Month 12. Updated version V2.0 delivered Month 20 V3.0 delivered Month 37

D3.1	Channel based random generators – interm. report	1.0	3	ICL	Techn	PU	T0+15	10/03/2014	Submitted Accepted	Yes	Initially planned Month 15. Version V1.0 delivered M 18.
D3.2	Channel based random generators – final report	1.0	3	TPT	Techn	PU	T0+36	30/11/2015	Submitted Accepted	Yes	delivered month 37.
D3.3	Coding techniques and algorithms for secrecy coding and secret key generation	1.0	3	ICL	Techn	PU	T0+36	05/11/2015	Submitted Accepted	Yes	delivered month 37.
D3.4	CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band	1.0 2.0	3	CEL	Techn	CO	T0+36	25/03/2016 21/11/2016	Submitted Accepted	Yes	Preliminary partial version at M 41. Final version with achieved experiments at M 48
D3.5	Simulations report of PHYSEC methods using measured CIR	1.0	3	TCS	Techn	CO	T0+42	04/12/2016	Submitted Accepted	Yes	written after availability of complete experimental results (D3.4) => delivered after M 48
D4.1	TRANSEC upgrades of existing RATs - study report	1.2 2.0	4	TCS	Techn	PU	T0+30	10/06/2015	Submitted Accepted	Yes	initial version V1.0 month 32. Updated V2.0 month 38
D4.2	TRANSEC upgrades of existing RATs – analyses & simulation complT report	1.2	4	TCS	Techn	PU	T0+36	30/11/2015	Submitted Accepted	Yes	Delivered month 37.
D4.3	NETSEC upgrades of existing RATs - study report	1.0	4	TCS	Techn	PU	T0+36	30/11/2015	Submitted Accepted	Yes	Delivered month 37.
D4.4	NETSEC upgrades of existing RATs - simulation analyses complements	1.0	4	TCS	Techn	PU	T0+42	30/08/2016	Submitted Accepted	Yes	Delivered month 46.
D4.5	New RATs and waveforms taking benefit of Physec upgrades – interim report	1.0	4	TCS	Techn	PP	T0+38	17/10/2016	Submitted Accepted	Yes	Delivered month 48. Includes security analysis by TCS's crypto-labo.
D4.6	New RATs and waveforms taking benefit of Physec upgrades – Final report	1.0 1.1	4	TCS	Techn	PP	T0+46	04/11/2016 18/11/2016	Submitted Accepted	Yes	Delivered shortly after month 48. Completes security analysis.
D5.1	WiFi test bed setup development report	1.0 1.1	5	CEL	Techn	PU	T0+36	20/03/2016 22/04/2016	Submitted Submitted Accepted	Yes	Initially planned Month 36. V1.0 M 41, upgraded V1.1 M 42
D5.2	WiFi test bed experimental campaign plant	1.α 1.0	5	CEL	Techn	PU	T0+34	24/03/2016 22/04/2016	Submitted Submitted Accepted	Yes	Initially planned Month 34. Draft Version V1.0 Delivered month 41. Final version delivered month 42.
D5.3	Intermediate Report on WiFi interceptor experiments with the test bed	1.0	5	CEL	Techn	PU	T0+38	29/03/2016 10/12/2016	Submitted Submitted Accepted	Yes	Initially planned Month 38. Draft Delivered month 41. Final V1.0 delivered after month 48.
D5.4	Final report on int. expe. on	1.0	5	CEL	Techn	PU	T0+44	15/12/2016	Submitted	Yes	V1.0 Delivered after month 48.

	test bed, with complementary simulation results. Final analysis on PHYSEC methods proof of concept								Accepted		
D5.5	Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades	1.0	5	CEL	Techn	PU	T0+46	20/12/2016	Submitted Accepted	Yes	V1.0 Delivered after month 48.
D6.1	Modeling of LTE-based cellular system Demo + simulation + report	1.0 2.0	6	VTT	Techn	PU	T0+24 T0+40	25/06/2015 19/02/2016	Submitted Accepted	Yes	Initially planned Month 24. V1.0 Delivered after restart at month 32. Upgraded at month 40.
D6.2	Simulation of interc. of waveform signals in LTE-based cellular system	1.0	6	VTT	Techn	PU	T0+42	12.05.2016	Submitted Accepted	Yes	None
D6.3	LTE-based cellular system simulations - Concluding report including simulation results and proposals for standardization	1.0	6	VTT	Techn	PU	T0+46	30.09.2016	Submitted Accepted	Yes	None

Figure 21: Table of deliverables

3.4.2- Milestones

The table below indicates the milestones of the reporting period that are specified in Annex I of the Grant agreement. This table is cumulative showing all milestones from the beginning of the project.

MS number qualification	Milestone name	WP(s) involved	Exp. date	Means of verification Status of deliverables
MS1 (major)	ManagT Plan. Consort. Agr.	WP1	Month 1	Deliverable D1.1 OK. CA signed
MS2 (major)	Planning of Dissemination Standardization	WP1	Month 3	Deliverables D1.6 OK and D1.9 OK
MS3 (major)	AB first orientations Threat CM and SP	WP1 WP2	Month 8	Deliverables D1.12 OK and D2.1 OK
MS4 (major)	Terminals' Security Architectures	WP2	Month 10	Deliverable D2.2 OK
MS5 (major)	PHYLAWS PPR (year 1) Status of WP2 Start of WP3 to WP6	WP1 WP2	Month 12	EC periodic meeting and report Deliverables D1.2 OK (PPR1), D1.6 OK, D1.9 OK, D1.12 OK Deliverables D2.1 OK, D2.2 OK, D2.3 OK
New DOW & schedule & Action Plan	WP1 WP3 to WP6	Month 20 June 2014	Action Plan Re-written DOW including new schedule Deliverable D2.4 completed Deliverable D3.1 completed New deliverable list and new delivery dates	
MS6 (major)	Mid project status	WP1 WP3, WP4 WP6	Month 32	Deliverables D1.7 OK; D1.10 OK Deliverables D2.4 OK; D3.1 OK; D4.1 OK; Deliverable D6.1 OK, D1.3 OK (PPR2 RM2)
MS7 (secondary)	Intermediate check of results over WPs with partners and Advisory Board members	WP1 WP3 to WP6	Month 35	Intermediate and final versions of reports being included in deliverable list of MS 8
MS8 (major)	PHYLAWS intermediate technical review PHYSEC Upgrades for existing and future standards Status WiFi Test bed Demo. Status of LTE simulation	WP1 WP3 WP4 WP5 WP6	Month 40	Deliverable D1.3 OK; D1.7 OK; D1.10 OK; D1.13 OK Deliverables D3.2 OK; D3.3 OK; D3.4 draft; Deliverables D4.2 OK, D4.3 OK; D4.5 postpned Deliverables D5.1; D5.2 draft; D5.3 draft Contribution to EC workshops, extra techn review D1.3a (QMR1 and PPR3) re-submission in progress
MS9 (secondary)	Intermediate Check of results over WPs with partners and Advisory Board members	WP1 WP3 to WP6	Month 46	Deliverable D1.14 D4.4 D6.2 Intermediate and final versions of reports being included in deliverable list of MS 10
MS10 (major)	PHYLAWS final review End of WP1 WP3 WP4 WP5 WP6 WiFi – Experimental Demo LTE – simulation Demo. Final Workshop (PIMRC'2016 W8 4 Sept 2016	WP1 WP3 WP5 WP6	Months 48 to 50	Project synthesis. Deliverables D1.8; D1.11, D1.14 Deliverable D3.5; Deliverables D4.6; Deliverables D5.4 and D5.5 Deliverable D6.3 RM4 and PPR4 Organization of a dedicated workshop. Deliverables D1.4 and D1.5

Figure 22: Table of Milestones

3.5- Use of the resources - Tables of (Cumulative) Person-Month Status and cost per Work Package

3.5.1- Recall of the initial WP and of the Person-Month planned use (extract from the new DoW)

Work packa-ge No	Work package title	Type of activity	Lead parti-cipant number	Lead partic. short name	Person months	Start month	End month
1	Management – Dissemination – Standardization	MGT	1	TCS	30	1	48
2	Requirements, completion of the state of the art, system analysis	RTD	1	TCS	44	1	20
3	Radio channels aspects of PHYSEC	RTD	2	TPT	77	6	42
4	New RATs and Wave forms for PHYSEC upgrades of future standards	RTD	1	TCS	43	25	46
5	Experimental study cases in 2.4 and 5 GHz bands – extraction and application of CIR – development of WiFi test bed	RTD	5	CEL	64	10	46
6	Simulation study case – LTE based cellular systems	RTD	4	VTT	38	12	46
	TOTAL				**296**		

3.5.2- Recall of the partners efforts (extract from the new DoW)

		Management Dissemination Standardization Advisory Board	Requirements, completion of the state of the art, system analysis	Radio channel aspects of PHYSEC	Introducing radio-channel randomness in existing and future RATs	Exp. study cases in 2.4 and 5 GHz bands Extraction and application of CIR Development of a WiFi test bed	Simulation study case – LTE based cellular systems	
Partner no.	**Partner short name**	**WP1**	**WP2**	**WP3**	**WP4**	**WP5**	**WP6**	**Total person months**
1	**TCS**	**20**	**12**	12	**28**	20	12	**104**
2	**TPT**	2	12	**26**	2	2	2	**46**
3	**ICL**	2	9	22	2	2	2	**39**
4	**VTT**	4	10	3	5	0	**22**(**)/ **26**(**)	**44**(**)/ **48**(**)
5	**CEL**	2	1	14	6	**40**	0	**63**
Total		**30**	**44**	**77**	**43**	**64**	**38**	**296**(**)/300(**)
Start month		1	1	1	25	10	12	
End month		48	20	42	46	46	46	

(**) In the initial VTT budget, cumulative PM for WP6 is 22 PM. With the budget readjustment requested in § 3.3.8, VTT would have 4 PM more in WP6, meaning that cumulative PM for WP6 would be 26 PM.

3.5.3- Person-Month use for the sub period M33-M38 compared to the planning of the sub-period revised at the end of the year2

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	used sub period 3 M33-M38	Planned sub period 3 M33-M38	used sub period 3 M33-M38	Planned sub period 3 M33- M38	used sub period 3 M33-M40	Planned sub period 3 M33-M38	used sub period 3 M33-M38	Planned sub period 3 M33-M38	used sub period 3 M33-M38	Planned sub period 3 M33-M38	used sub period 3 M33-M38	Planned sub period 3 M33-M38	Used sub period 3 total M33-M38	Planned sub period 3 total M33-M38
Beneficiary 1 TCS = Coordinator	7(*)	3	0	0	1	1	6	6	4	4	4	4	22 (*)	18(*)
Beneficiary 2 TPT	0.15	0.2	0	0	1.4	1	0	0	0.5	1	0.2	0.5	2.25	2.7
Beneficiary 3 ICL	0	0	0	0	9	9	0	0	0	0	0	0	9	9
Beneficiary 4 VTT	0.4	0.4	0	0	1	1	2.6	3	0	0	7.8(**)	7	11.8(**)	11.4
Beneficiary 5 CEL	1	1	0	0	4	4	1	1	16	16	0	0	22	22
TOTAL	8.55(*)	4.6(*)	0	0	16.4	16	9.6	10	20.5	21	12	11.5	67.05	63.1

(*) = PM exceeds compared to planned effort, because of standardization intensive effort + excessive energy and time for WP5 advancement and report review.
(**) = PM exceeds compared to planned effort, because of the need to design band-limited tag signals that would meet spectrum emission mask requirements.
Used Year 3 sub period M33-M38 = number of person months consumed at the start of period 3
Planned Year 3 sub period M33-M38 = total effort planned for the project in the latest version of the description of work - annex I to the grant agreement

3.5.4- Person-Month use during the sub period M39-M41 compared to the planning of the sub-period revised at the end of the preceding

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	used sub period M39-M41	Planned sub period M39-M41	used sub period M39-M41	Planned sub period M39-M41	used sub period M39-M41	Planned sub period M39-M41	used sub period M39-M41	Planned sub period M39-M41	used sub period M39-M41	Planned sub period M39-M41	used sub period M39-M41	Planned sub period M39-M41	Used sub period total M39-M41	Planned sub period total M39-M41
Beneficiary 1 TCS = Coordinator	3(*)	1	0	0	1	1	2	2	2	2	1,5	1,5	9.5 (*)	7.5(*)
Beneficiary 2 TPT	0.1	0.1	0	0	0	0	0	0	0.6	1	0.15	0.5	0.85	1.6
Beneficiary 3 ICL	0	0	0	0	3	3	0	0	0	0	0	0	3	3
Beneficiary 4 VTT	0.4	0.4	0	0	1	1	0	0	0	0	3.2	2	4.6(**)	3.4
Beneficiary 5 CEL	1	1	0	0	2	2	1	1	4	4	0	0	8	8
TOTAL	4.50(*)	2.5(*)	0	0	7.0	7.0	3	3	6.6	7	4.85	4	25.95	23.5

(*) = PM exceeds compared to planned effort, because of standardization intensive effort + excessive energy and time for WP5 advancement and report review.
(**) = PM exceeds compared to planned effort, because of the need to design band-limited tag signals that would meet spectrum emission mask requirements.
Used sub period M39-M41 = number of person months consumed at sub period M39-M41 of year 3
Planned sub period M39-M41 = total effort planned for the project in the latest version of the description of work

3.5.5- Person-Month use during the sub period M42-M44 compared to the planning of the sub-period revised at the end of the preceding

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	used sub period M42-M44	Planned sub period M42-M44	used sub period M42-M44	Planned sub period M42-M44	used sub period M42-M44	Planned sub period M42-M44	used sub period M42-M44	Planned sub period M42-M44	used sub period M42-M44	Planned sub period M42-M44	used sub period M42-M44	Planned sub period M42-M44	Used sub period total M42-M44	Planned sub period total M42-M44
Beneficiary 1 TCS = Coordinator	2(*)	1	0	0	0.5	0	2	2	1.5	2	1	1	7 (*)	6.0(*)
Beneficiary 2 TPT	0.1	0.1	0	0	0	0	0	0	0.2	1	0.1	0.5	0.4	1.6
Beneficiary 3 ICL	0	0	0	0	0	0	1	1	1	1	0	0	2	2
Beneficiary 4 VTT	0	0	0	0	0	0	0	0	0	0	2	2	2(**)	2
Beneficiary 5 CEL	0	0	0	0	0	0	0	0	6	6	0	0	6	8
TOTAL	2.1(*)	1.1(*)	0	0	0.5	0.0	3	3	8.7	10	3.1	3.5	17.4	19.6

(*) = PM exceeds compared to total planned effort, because of standardization intensive effort + excessive energy and time for WP5 advancement and report review.
(**) = PM exceeds compared to total planned effort, because of the need to design band-limited tag signals that would meet spectrum emission mask requirements.
Used sub period M42-M44 = number of person months consumed at sub period M42-M44 of year 3
Planned sub period M42-M44 = total effort planned for the project in the latest version of the description of work

3.5.6- Person-Month use for the sub period M45-M48 compared to the revised planning of the sub-period at the end of the preceding one

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	used sub period M45-M48	Planned sub period M45-M48	used sub period M45-M48	Planned sub period M45-M48	used sub period M45-M48	Planned sub period M45-M48	used sub period M45-M48	Planned sub period M45-M48	used sub period M45-M48	Planned sub period M45-M48	used sub period M45-M48	Planned sub period M45-M48	Used sub period total M45-M48	Planned sub period total M45-M48
Beneficiary 1 TCS = Coordinator	8(*)	2.5	0	0	6	0	4	1	3.5	0.5	0.5	0	22 (*)	4(*)
Beneficiary 2 TPT	0.4	0.5	0	0	0	0	0	0	0.25	0.25	0.05	0.25	0.7	1
Beneficiary 3 ICL	0.1	0	0	0	0	0	0.5	0.5	0.25	0.25	0.25	0.25	1.1	1
Beneficiary 4 VTT	0.5	0	0	0	0.28	0	1.98	1.7	0	0	2.67	1	5.43(**)	2.7(**)
Beneficiary 5 CEL	1	1	0	0	3	0	0	0	6	6	0	0	10	7
TOTAL	10.0 (*)	4 (*)	0	0	9.28	0	6.48	3.2	10	7	3.47	1.5	39.23	15.7

(*) = PM exceeds compared to total planned effort, because of standardization intensive effort + excessive energy and time for WP3+5 advancement and report review.

(**) = PM exceeds compared to total planned effort, because of the need to design band-limited tag signals that would meet spectrum emission mask requirements and additional simulations of secrecy coding schemes.

Used sub period M45-M48 = number of person months consumed at sub period M42-M44 of year 3

Planned sub period M45-M48 = total effort planned for the project in the latest version of the description of work

3.5.7- Person-Month use for the period 3 M33-M48 compared to the planning of the period3 revised at the end of the period 2

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	used period 3 M33-M48	Planned period 3 M33-M48	used period 3 M33-M48	Planned period 3 M33-M48	used period 3 M33-M48	Planned period 3 M33-M48	used period 3 M33-M48	Planned period 3 M33-M48	used period 3 M33-M48	Planned period 3 M33-M48	used period 3 M33-M48	Planned period 3 M33-M48	Total used Period 3 M45-M48	Total planned Period 3 M45-M48
Beneficiary 1 TCS = Coordinator	20(*)	8	0	0	8.5	13	15	9	11	6	7	11	61.5 (*)	35.3(*)
Beneficiary 2 TPT	0.5	0.1	0	0	0	0	0	0	1.55	2	1.5	1.4	3.55	3.4
Beneficiary 3 ICL	0.1	0	0	0	12	6	1.5	2	1.25	2	0.25	2	15.1	12
Beneficiary 4 VTT	1.4	0.8	0	0	2.28	2	4.58	4.7	0	0	15.67	12	23.93(**)	14(**)
Beneficiary 5 CEL	0.6	0.5	0.2	0	4.8	4.6	3	2.8	34.2	29.5	0	0	42.8	37.4
TOTAL	22.6(*)	9.4(*)	0.2	0	27.58	25.6	24.08	18.5	48.00	39.5	24.42	26.4	146.88	102.1

(*) = PM exceeds compared to total planned effort, because of standardization intensive effort + excessive energy and time for WP3+4+5 advancement and report review.

(**) = PM exceeds compared to total planned effort, because of the need to design band-limited tag signals that would meet spectrum emission mask requirements and additional simulations of secrecy coding schemes.

Used sub period M45-M48 = number of person months consumed at sub period M42-M44 of year.

Planned sub period M45-M48 = total effort planned for the project in the latest version of the description of work

3.5.8- Person-Month use at the end of the project (M 48): cumulative actual per WP versus total use planned effort at the project's start.

Workpackage	WP1		WP2		WP3		WP4		WP5		WP6		TOTAL per Beneficiary	
	Actual	Planned Total	Actual	Planned Total	Actual	Planned Total	Actual	Planned Total	Actual	Planned Total	Actual	Planned Total	Actual total	Planned total
Beneficiary 1 TCS = Coordinator	30(*)	20	12.5	12	16.4(*)	12	34(*)	28	22(*)	20	8.3	12	123.2(*)	104
Beneficiary 2 TPT	2.65	2	11.6	12	27.62	26	2.25	2	1.55	2	1.12	2	46.15	46
Beneficiary 3 ICL	2.1	2	8.9	9	28.02	22	1.5	2	1.25	2	0.25	2	42.02	39
Beneficiary 4 VTT	4.13	4	10.59	10	3.02	3	5.2	5	0	0	27.67	22(**)/ 26(**)	50.61(**)	44(**)/ 48(**)
Beneficiary 5 CEL	2.1	2	1.2	1	14.2	14	6.2	6	44.7	40	0	0	68.4	63
TOTAL	40.74	30	44.79	44	87.86	77	49.15	43	69.50	64	38.34	38	330.38	296(**) 300(**)

Actual at M48 = number of person months consumed from the beginning of the project to the end of period3 **plus month 49 and 50 (November and December)**

Planned total = total effort planned for the project in the latest version of the description of work - annex I to the grant agreement

(*) = PM exceeds compared to total planned effort, because of standardization intensive effort + excessive energy and time for WP3+4+5 advancement and report review.

(**) In the initial VTT budget, cumulative PM for WP6 is 21.8 PM out of 22 PM, with the budget readjustment requested in § 3.3.8, VTT would have 4 PM more in WP6, meaning that cumulative PM for WP6 would be 21.8 PM out of 26 PM.

3.6- Explanation of the use of the resources and financial statements

3.6.1- TCS

PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 1 (TCS) FOR THE PERIOD 1.07.2013 – 31.10.2016			
Work Package	Item description	Amount in € with 2 decimals	Explanations
RTD, WP3, WP4, WP5, WP6,	Personnel direct costs	162,116 €	Total declared salaries is 23.9 PM shared among WP3 : 8.5 PM – R. Molière, C Kameni, F. Delaveau WP4 : 9 PM – C Kameni, R. Molière, F. Delaveau WP5 : 4.5 PM – C Kameni, F. Delaveau WP6 : 1.9 PM – C Kameni, F. Delaveau
RTD, WP3, WP4, WP5, WP6,	Other direct travel cost	6,636 €	Consortium technical meeting and review technical meetings in Brussels for R. Molière, C Kameni, F. Delaveau (08-10 Sept 2015 - 29-31 Mar 2016 – 21 Dec 2016).
RTD	Indirect costs	132,206 €	TCS indirect Cost relevant to RTD
RTD	Total RTD	300,958 €	Total expenditure RTD
RTD	Requested Funding @ 50% reduced to max EC contribution	150,479 €	Claim expenditure RTD
MGT WP1	Personnel Costs	129,208 €	Total declared salaries is 15.4 PM shared among F. Delaveau, R. Molière, C. Kameni
MGT WP1	Subcontracting	7,500 €	Certification on financial statements
MGT WP1	Other Direct travel Costs	63,380 €	Travelling costs relevant to WP1 T1.3 “standardization” WP1 T1.4 Advisory Board invitation, WP1 T1.2 “dissemination” (including the final workshop at PIMRC’2016 Valencia with relevant registrations and invitations).
MGT	Indirect costs	105,370 €	Indirect Cost relevant to MGT
WP1	Total MGT	305,458 €	Total expenditure MGT
MGT	Requested funding @ 100% reduced to max EC contribution	305,458 €	Claim expenditure MGT
TOTAL COST		**606,416 €**	
TOTAL REQUESTED FUNDING		**455,937 €**	

3.6.2 TPT

PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 2 (TPT) FOR THE PERIOD 1.07.2013 – 31.10.2016			
Work Package	Item description	Amount in € with 2 decimals	Explanations
RTD, WP3, WP4, WP6,	Personnel direct costs	28,051.00€	TOTAL PM = 2.26 WP3 TOTAL 0.67 PM (2 Professors) WP4 TOTAL 1.18 PM (2 professors) WP6 TOTAL 0.41 PM (1 professor)
RTD WP5	Travel costs	1,688 €	Working meeting with Prof.Cong-Ling (Imperial college London) 15-28 Nov 2015 in London (De Andrade Campello Junior Antonio Carlos)
RTD WP2 WP3	Other direct costs	1,281 €	Equipment Depreciation WP3 and WP5 : 403 € 1 PC OPTIPLEX 7010 WP5 : 359 € 1 PRECISION T3600 WP5 : 519 € 1 LATITUDE E6230
RTD	Indirect costs	18,612 €	Indirect Cost relevant to RTD
RTD	Total RTD	49,632 €	Total expenditure RTD
RTD	Requested funding @ 75% reduced to max EC contribution	37,224 €	Claim expenditure RTD
MGT WP1	Personnel and direct costs	11,292 €	Personnel costs TOTAL PM = 0.87 (1 Professor)
MGT WP1	Travel costs	1314 €	PHYLAWS Review 08-10 Sept 2015 in Brussels (A Sibille, JC Belfiore) PHYLAWS Review 29-31 Mar 2016 in Brussels (A. Sibille) IRACON 2nd MC meeting and 1st technical meeting 31 May-01 Jun 2016 in Lille (Telecom Lille) (A Sibille)
MGT WP1	Other direct costs	1,140 €	Equipment Depreciation WP1 : 465 € 1 LATITUDE E6230 WP1 : 675 € 1 Precision Tower 5810
MGT WP1	Indirect costs	8,247 €	Indirect Costs relevant to MGT
MGT WP1	Total MGT	21,993.00 €	Total expenditure MGT
MGT WP1	Requested funding @ 100% reduced to max EC contribution	21,993.00 €	Claim expenditure MGT
TOTAL COST		**71,625.00 €**	
TOTAL REQUESTED FUNDING		**59,217.00 €**	

3.6.3- VTT

PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 4 (VTT OY) FOR PERIOD 1.07.2015 – 31.10.2016			
Work Package	Item description	Amount in € with 2 decimals	Explanations
RTD: WP3, WP4, WP6	Personnel costs	136,182.00 €	WP3: Total 1.28 PM (2 Senior scientists). WP4: Total 4.58 PM (3 Senior scientists). WP6 : Total 13.67 PM (3 Senior scientists).
WP6	Use of a special equipment	1,200.00 €	Use of MATLAB licence
RTD: WP3, WP4, WP6	Travel costs	1,904.00 €	3GPP/SA3 standardization meeting for disseminating results from PHYLAWS 23.-27.5.2015 in Tallinn, Estonia: J. Suomalainen (642 €) PHYLAWS AB-meeting and project meetings 19.-21.1.2016 inParis, France: S. Boumard (1217 €) Mathworks seminar on the se of LTE Toolbox 17.3.2016 in Espoo, Finland: A. Kotelba (45 €)
RTD	Indirect costs	110,745.00 €	Indirect Costs on RTD
RTD	Total costs RTD	259,031.00 €	Total expenditure MGT
RTD	Requested funding @ 75% reduced to max EC contribution	194,273 €	Claim expenditure RTD
MGT: WP1	Personnel costs	6,474.00 €	Total 0.9PM (2 Senior scientists, 1 Research team leader).
MGT: WP1	Travel costs	5,983.00 €	PHYLAWS Y2 review meeting and project´s technical meeting 8.-11.9.2015 in Brussels, Belgium: A. Kotelba (701 €) Meeting with AB of PHYLAWS 19.-22.1.2016 in Paris, France : A. Kotelba (648 €) PHYLAWS technical and review meetings 29-31.3.2016 in Brussels, Belgium: A. Kotelba and S. Boumard (1,846 €) PHYLAWS workshop and partner meeting 2-6.9.2016 in Valencia, Spain: A. Kotelba and S. Boumard (2,788 €).
MGT - WP1	Subcontacting	1,157.00 €	Certification on financial statements
MGT - WP1	Indirect costs	5,962.00 €	Indirect Costs relevant to MGT
MGT - WP1	Total costs MGT	19,306.00 €	Total expenditure MGT
MGT - WP1	Requested funding @ 100 % reduced to max EC contribution	19,306.00 €	Claim expenditure MGT
TOTAL COSTS		**278,337.00 €**	
TOTAL REQUESTED FUNDING		**213,579.00 €**	

3.6.4- ICL

PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 3 (ICL) FOR THE PERIOD 1.07.2013 – 31.10.2016			
Work Package	Item description	Amount in € with 2 decimals	Explanations
RTD: WP3	Personnel direct costs	47,250.00 €	Total WP3 = 11.99 PM : Dr Z. Wang (11 PM), Dr C Ling (0.99 PM).
RTD: WP4	Personnel direct costs	11,720.00 €	Total WP4 = 2.86 PM : Mr S Lyu (2.86 PM)
RTD: WP5	Personnel direct costs	1,091.00 €	Total WP5 = 0.16 PM : Dr C Ling (0.16 PM).
RTD: WP6	Personnel direct costs	1,182.00 €	Total WP6 = 0.16 PM : Dr C Ling (0.16 PM).
RTD WP2 WP3 WP4 WP5 WP6	Other direct Costs	6,521.00 €	Travel costs Attending project meetings: PPR2 (Travel, hotel and subsistence at PHYLAWS EC Year2 Meeting, 8th - 10th September 2015, Brussels, Dr Z Wang (307 €) Phylaws meeting, Paris, 21-22 May 2015 Dr Cong Ling (437 €) Phylaws meeting, Paris, 05 Nov. 2015 Mr Ling Liu (375 €) AB Second meeting: Travel and hotel for Paris, 19-20 Jan 2016, Paris, Dr Cong Ling (376 €) Intermediate review meeting PPR3 Meeting, Brussels,29-30 March 2016 Dr L Cong & Dr Z Wang (810 €) Dissemination Dr Z Wang – ISIT Meeting, Hong Kong, 13-20 June 2015 (1684 €) Dr C ling & Dr Z Wang – ISIT Meeting, Barcelona, 10-15 July 2016 (887 €) Dr C Ling - Workshop on number theory, York, 5-7July 2016 (225 €) Dr C Ling - Turbo Codes Symposium, Brest, France, 5-9 Sept. 2016 (845 €) Dr C Ling -Theory Workshop, Cambridge, 11 to 14, Sept. 2016 (575 €)
RTD	Indirect Costs @ 60%	40,658.00 €	Indirect Costs relevant to RTD
RTD	TOTAL RTD EXPENDITURE	108,422.00 €	Total expenditure RTD
RTD	Requested funding @ *75%* reduced to max EC contribution	81,316.00 €	Claim expenditure RTD
MGT- WP1		0.00 €	
MGT- WP1	Indirect Costs @ 60%	0.00 €	Indirect Costs relevant to MGT
MGT- WP1	TOTAL MGT EXPENDITURE	0.00 €	Total expenditure MGT
MGT- WP1	Requested fund. @ *100%* reduced to max EC contribution	0.00 €	Claim expenditure MGT
TOTAL COSTS		**108,422.00 €**	
TOTAL REQUESTED FUNDING		**81,316.00 €**	

3.6.5- CEL

PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 5 (CEL) FOR THE PERIOD 1.07.2013 – 31.10.2016			
Work Package	Item description	Amount in € with 2 decimals	Explanations
RTD, WP3, WP4, WP5,	Personnel direct costs	409,647 €	Total = 42.9 PM WP3 = 5.0 PM – 3 engineers WP4 = 3.1 PM – 3 engineers WP5 = 34.8 PM – 6 engineers
RTD, WP3, WP4, WP5,	other direct travel costs	9,292 €	Brussels 9/2015, Paris 1/2016, Brussels 3/2016, Valencia 9/2016, Brussels 12/2016
	Other direct costs	34,630 €	DCEVA FPGA & JBOX, Dini boards, 6GHz QFN 88PIN Socket, Temperature chamber, RF Shield box, PCIe GEN 2 PROTOCOL TEST, IQxel -160 Test system
RTD	Indirect cost @ 60%	272,141 €	Indirect Costs relevant to RTD
RTD	Total RTD	725,710 €	Total expenditure RTD
RTD	Requested Funding @ 75% reduced to max EC contribution	544,282 €	Claim Expenditure RTD
MGT	Personnel Costs	8,700 €	Total = 0.6 PM - Project Manager Ronny Barak and Nir Shapira
MGT	Subcontracting	3,632 €	Cost of CFS audit
MGT	Other direct cost	1,362 €	Travel costs for consortium management meeting of Mr Nir Shapira: PHYLAWS final review Brussels 12/2016.
MGT	Indirect costs @ 60%	6,037 €	Indirect Costs relevant to MGT
MGT	Total MGT	19,731 €	Total expenditure MGT
MGT	Requested Funding @ 100% reduced to max EC contribution	19,731 €	Claim Expenditure MGT
TOTAL COSTS		**745,441 €**	
TOTAL REQUESTED FUNDING		**564,013 €**	

Annex 1: Agenda and conclusion of the final (Brussels, 2016-12-21)

We propose below an agenda for the final review of period 3, to be held in Brussels on December 21 2016. The purpose of this final review is

- to recall about the Physec-based secure schemes developed into the Phylaws project
- to demonstrate simulations enabling Secret key Generation and Secrecy Coding that were developed by the Phylaws partners, and present overall results of simulation activities (WP6);
- to demonstrate Wifi test bed enabling Secret key Generation and Secrecy Coding that were developed by the Phylaws partners, and present results of experimentation activities (WP5);
- to focus on last developments and on the security analysis of the Physec–based secured schemes achieved during the project (Secure Pairing, Secret key generation, Secrecy Coding), when facing nominal threats and when facing ultimate threats
- to recall results of academic tasks and relevant measurements (WP3) and developments (WP4);
- to focus on the results of standardization actions, that were very intensive during the last period of the project
- to focus on the results of dissemination, including the dedicated workshop that held in PIMRC'2016, the preparation of journal papers and book chapters
- to present a brief recall on Advisory Board activities
- to present a brief recall on IPRs,
- To present the final status and results of management activities, including a brief recall of thje project history, a short presentation of all deliverables, risk management and Ethical issues

This agenda proposal and the conclusion slides of the PPR4 review are included in the PowerPoint files attached hereafter:

Annex 2: Deliverable list of the Phylaws project

See the attached file below

WORK PACKAGE 1

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 1.1	Kick-Off meeting. Management Plan, including risk evaluation, analysis of Ethical Issues. Minutes of K.O. Consortium Agreement.	WP 1.1	R	PU
D 1.2	Months 1-12 (year1) review meeting RM1 and PPR1	WP 1.1	R	PU
D 1.3	Months 13-31 review meeting RM2 and PPR2	WP 1.1	R	PU
D 1.3a	Extra technical review meeting RM3 and PPR3	WP 1.1	R	PU
D 1.4	Synthesis of the project management. Final release of Risk analysis. Final report on Ethical Issues	WP 1.1	R	PU
D 1.5	Months 32-48 review meeting RM4 and PPR4 – Synthesis – Open workshop on projects results	WP 1.1	R	PU
D 1.6	Dissemination planning report	WP 1.2	R	PU
D 1.7	Dissemination intermediate report	WP 1.2	R	PU
D 1.8	Dissemination final report	WP 1.2	R	PU
D 1.9	Standardization planning report	WP 1.3	R	PU
D 1.10	Standardization interm. Report	WP 1.3	R	PU
D 1.11	Standardization final report	WP 1.3	R	PU
D 1.12	Advisory board meeting report 1	WP 1.4	R	PU
D 1.13	Advisory board meeting report 2	WP 1.4	R	PU
D 1.14	Advisory board meeting report 3	WP 1.4	R	PU

WORK PACKAGE 2

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 2.1	Analysis of the threat counter-measure and protection techniques in existing and new standards – report	WP 2.1	R	PU
D 2.2	Security architectures in wireless terminal – report	WP 2.2	R	PU
D 2.3	Fundamental aspects of physical layer security – report	WP 2.3	R	PU
D 2.4	New opportunities provided by modern wave forms and sensing/measure of radio environments – report	WP 2.4	R	PU

WORK PACKAGE 3

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 3.1	Channel based random generators – interm. report	WP 3.1	R	PU
D 3.2	Channel based random generators – final report	WP 3.1	R	PU
D 3.3	Coding techniques and algorithms for secrecy coding and secret key generation	WP 3.2	R	PU
D 3.4	CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band	WP 3.3	R	CO
D 3.5	Simulations report of PHYSEC methods using measured CIRs	WP 3.4	R	CO

WORK PACKAGE 4

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 4.1	TRANSEC upgrades of existing RATs - study report	WP 4.1	R	PU
D 4.2	TRANSEC upgrades of existing RATs - simulation and analyses complements	WP 4.1	R	PU
D 4.3	NETSEC upgrades of existing RATs - study report	WP 4.2	R	PU
D 4.4	NETSEC upgrades of existing RATs - simulation analyses complements	WP 4.2	R	PU
D 4.5	New Rats and Wave Forms taking benefit of Physec upgrades – interim report	WP 4.3	R	PP
D 4.6	New Rats and Wave Forms taking benefit of Physec upgrades – final report	WP 4.3	R	PP

WORK PACKAGE 5

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 5.1	WiFi test bed setup development report	WP 5.1	R	PP
D 5.2	Experiment campaign plan	WP 5.2	R	PP
D 5.3	Intermediate Report on WiFi interceptor experiments with the test bed	WP 5.3	R	PU
D 5.4	Final report on interception experiments on test bed, synthesized with complementary simulation results. Final analysis on PHYSEC methods proof of concept	WP 5.4	R	PU
D 5.5	Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades	WP 5.5	R	PU

WORK PACKAGE 6

Del. N°	Deliverable name	WP or task N°	Nat	Diss. level
D 6.1	Modeling of LTE-based cellular system Demo + simulation + report	WP 6.1	R	PU
D 6.2	Simulation of interception of waveform signals in LTE-based cellular system	WP 6.2	R	PU
D 6.3	LTE-based cellular system simulations – Concluding of the work package and proposals for standardization	WP 6.3	R	PU