ETSI Security Week

2nd 5G-ENSURE Project Workshop

15 June, 2017, Sophia Antipolis

09:15-10:15	**5G-ENSURE Achievements**
	5G-ENSURE Project Overview, Luciana Costa, TIM
	Trust Model for 5G, Mike Surridge, IT INNOVATION
	Risk Model, Linas Maknavicius, Nokia
	5G Security Architecture, Alireza Ranjbar, Ericsson
10:15-11:00	**Security Enablers for 5G Network**
	Privacy Enablers: Enhanced Identity Protection, Madaline Baltatu, TIM
	Network Management and Virtualisation Isolation Security, Felix Klaedtke, NEC
	Bootstrapping Trust in Virtualised Network Environments, Nicolae Paladi, SICS
11:00	***Networking Coffee Break***

11:00	***Networking Coffee Break***
11:30-12:45	**Security: the work of standardization and 5G-PPP Cooperation**
	"What else needs to be done on 5G Security?" - A walk through our Open Consultation, Luciana Costa, TIM
	5G-ENSURE Standardisation Plan, Paolo De Lutiis, TIM
	5G Security: Phase 1 Landscape, Jean Philippe Wary, Orange
	3GPP 5G Security Work, Anand R. Prasad, NEC
	IoT Scenarios and Standardisation, Giovanni Bartolomeo, University of Rome
12:45-13:30	**International panel on 5G Security way forward**
	What work needs to be done over the next few years towards the integration and uptake of 5G security solutions as we move towards the launch of the first commercial 5G networks? International security experts and 5G-ENSURE advisory board members discuss priority actions for standardisation, security and co-operation as key to building consensus. **Panelists** Anand Prasad, Chairman 3GPP SA3 Charles Brookson, Chair ETSITC CYBER Jovan Golic, lead NGMN Security Competence Team, Telecom Italia Roberto Cascella, European Cyber Security Organisation (ECSO)
13:30	***Networking Lunch and Refreshments***

5G-ENSURE
Project Overview

pascal.bisson@thalesgroup.com
luciana.costa@telecomitalia.it

2017-06-16

Agenda

- 5G Security Use Cases
- 5G Security Architecture
- 5G Security Technical Roadmap
- 5G Security Enablers
- 5G Security Testbed
- 5G Security Standardisation

5G Security Use Cases

- Hundreds of use-cases have been defined by 3GPP, other 5G-PPP projects, NGMN, etc
- Very few on security
  - Security aspects may be implicit, but not in focus
- 5G-ENSURE defined additional use-cases aiming to illuminate 5G security issues

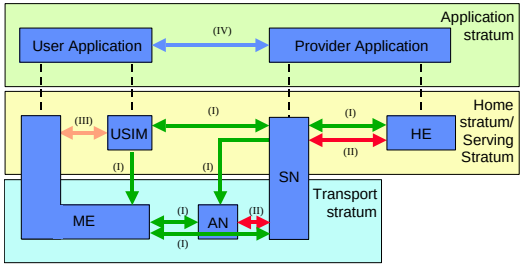
Results

- Deliverable D2.1 - Use Cases
- Defines 31 use-cases, grouped in 11 clusters
  - 2-6 uses-cases per cluster

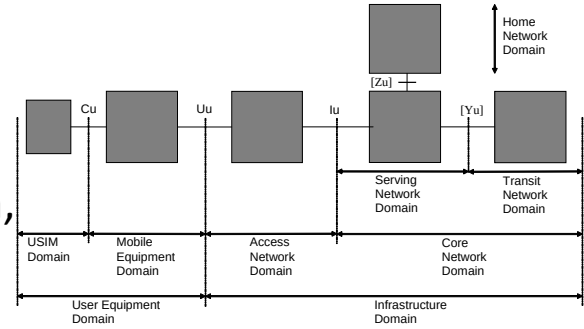
1. Identity management
2. Enhanced Identity protection and authentication
3. IoT device authentication & key management
4. Authorization of device-to-device communication
5. SDN, virtualization & monitoring
6. Radio Interface Protection
7. Mobility Management Protection
8. Ultra-reliable & standalone operation
9. Trusted core & interconnect
10. 5G Enhanced security services
11. Lawful interception

5G Security Architecture

- Leverages on current 4G Security Architecture (TS 33.401) is thus built on “strata” and “domains” (from TS 23.101)



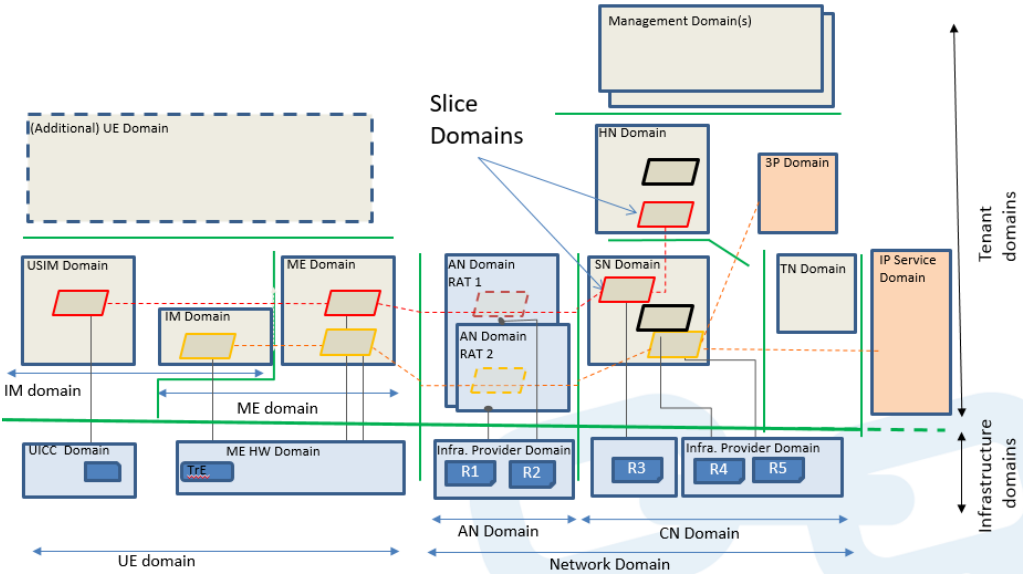
- Aims to address major gaps (e.g. Trust model) and differences introduced by 5G
  - Multi-access (e.g. 3GPP + WLAN)
  - Re-use outside telco (e.g. industry automation)
  - Non-physical architecture, building on cloud/virtualization, network slicing
  - Management/orchestration has central role
  - …



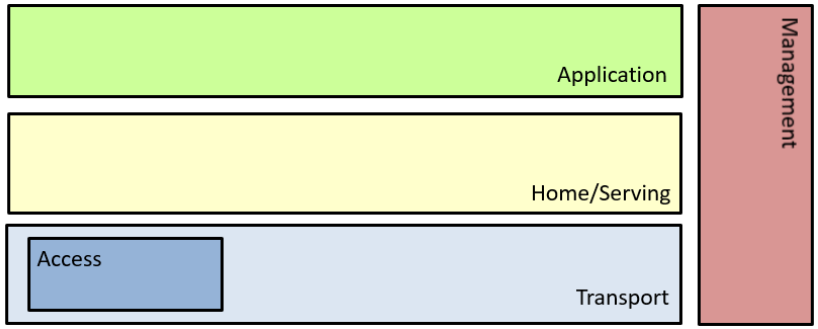
- Cover key modifications requested for 5G
  - Capture virtualization and network slicing
    - Distinguish physical vs logical/functional domains
  - Place management/orchestration on the map
  - Non-telco actors
    - Add new domains

Our Security Architecture is built from

Our 5G (Security) Domains



5G Strata



The Management Stratum contains, e.g.
- "SNMP-type" management
- Orchestration
- Security management (monitoring, key distribution etc)

Security feature groups (not covered here)

Rationale is to re-use well-known concepts, extending to 5G security landscape

More details: Deliverable D2.4 - Security Architecture (draft)

5G Security enablers

- Focused on areas of *major* concerns:
  - **Authentication, Authorization and Accounting**
  - **Privacy**
  - **Trust**
  - **Security Monitoring**
  - **Network Management & Virtualization isolation**

- Aim at addressing security requirements identified for 5G to generate the necessary Trust & Confidence and make its promises

5G Security enablers

- Come with:
  1. A “Product vision” detailing the features to be offered as well as their scheduling over the 2 releases (R1/Sep’16 vs R2/Aug’17)

     Full details available in latest version of Technical Roadmap: Deliverable D3.5: 5G PPP security enablers technical roadmap (Update)

  2. Open specifications

  3. A reference implementation (for those developed) conformant to the open specifications and accompanying documentation
     - As such most of them are software released (either close or open source as per decision taken by enabler owner)

Security enablers technical roadmap (D3.5)

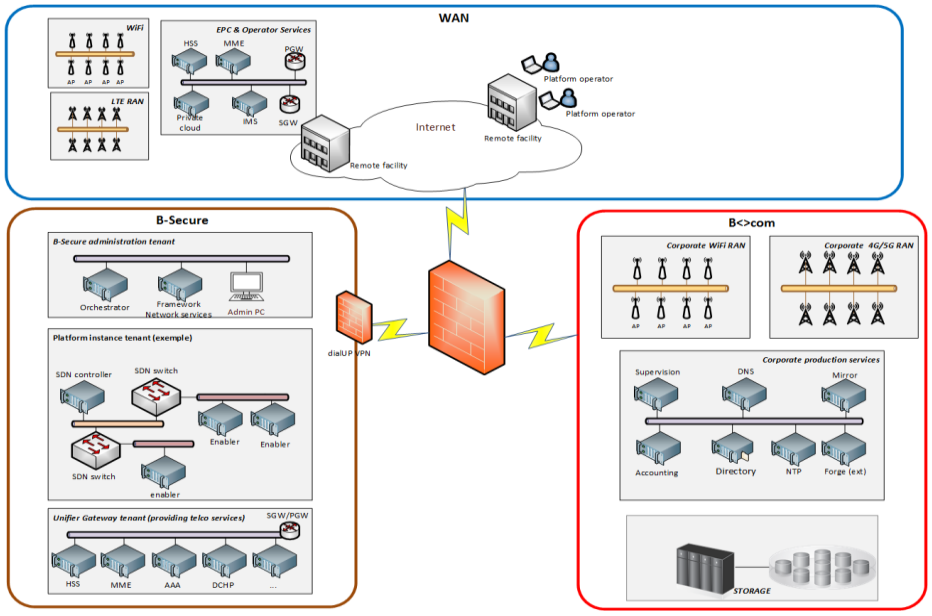
Category	Security enabler Name	Security features	
		R1 features (achieved)	R2 features (planned)
AAA	Basic AAA enabler	Forward Secrecy (early specification) AAA aspects of trusted micro-segmentation (early specification)	Forward Secrecy AAA aspects of trusted micro-segmentation Trusted interconnect and authorization
	IoT	*Group authentication by extending the LTE-AKA protocol* *vGBA*	Group-based AKA continued (focus on PFS, OAI impl.) Non-USIM based AKA Bring Your Own Identity (BYOI)
	Fine-grained Authorization Enabler	*Basic Authorization in Satellite systems* *Basic Distributed Authorization Enforcement for RCDs*	AAA integration with satellite systems Authorization and authentication for RCD based on ongoing IETF standardization
	Federative authentication context usage	*none*	Storage of authentication level Usage of authentication level
Privacy	Privacy Enhanced Identity Protection	*Encryption of Long Term Identifiers (IMSI KP-ABE-based)*	Home Network centric IMSI protection IMSI Pseudonymization
	Device Identifiers Privacy	*Enhanced privacy for network attachment protocols*	Anonymous and optimised address selection for network attachment
	Device-based Anonymization	*none*	Format preserving anonymization algorithm Privacy configuration
	Privacy Policy Analysis	*none*	privacy policy specification privacy preferences specification comparison of policies and preferences
Trust	Trust Builder	*5G asset model v1* *Graphical modelling tool v1*	5G asset model v2 Graphical modelling tool v2 5G threat and trust knowledgebase
	Trust Metric Enabler	Trust metric based network domain security policy management	Improved trust metric based on extended data
	VNF Certification	VNF Trustworthiness Evaluation	VNF Trustworthiness Certification
	Security Indicator	none	Security indicator subscriber display
	Reputation based on Root Cause Analysis for SDN	none	Root Cause Analysis for SDN
Security monitoring	System Security State Repository	Deployment model ontology (also known as 5G asset model)	System Security State Repository service
	Security Monitor for 5G Micro-Segments	Complex Event Processing Framework for Security Monitoring and Inferencing	Risk-based adaptation of micro-segments Extended data gathering Cross-domain information exchange
	PulSAR: Proactive Security Analysis and Remediation	5G specific vulnerability schema	5G specific vulnerability schema implementation PulSAR interface with Generic Collector
	Satellite Network Monitoring	Pseudo real-time monitoring v1 Threat detection	Pseudo real-time monitoring v2 Active security analysis Pre-emptive mitigation security actions
	Generic Collector Interface (GCI)		integration within others monitoring enablers
Network Management and Virtualization Isolation	Anti-Fingerprinting	Controller-Switch-Interaction Imitator	no further release
	Access Control Mechanisms	Southbound Reference Monitor v1	Southbound Reference Monitor v2 Access Requirements for VNF Container Resources
	Component-Interaction Audits	Basic OpenFlow Compliance Checker v1	Basic OpenFlow Compliance Checker v2 Basic NFV Reconfiguration Compliance Checker
	Micro-segmentation	Dynamic arrangement of Micro-Segments	Extended Northbound API Support for multi-domain micro-segments
	Bootstrapping Trust	Integrity Attestation of virtual switches v1	Integrity Attestation of virtual switches v2 Integrity Attestation of VNFs running in Docker containers
	Flow Control		Detection of malicious behaviours in virtual networks In-network threat mitigation for critical functions in virtual networks.

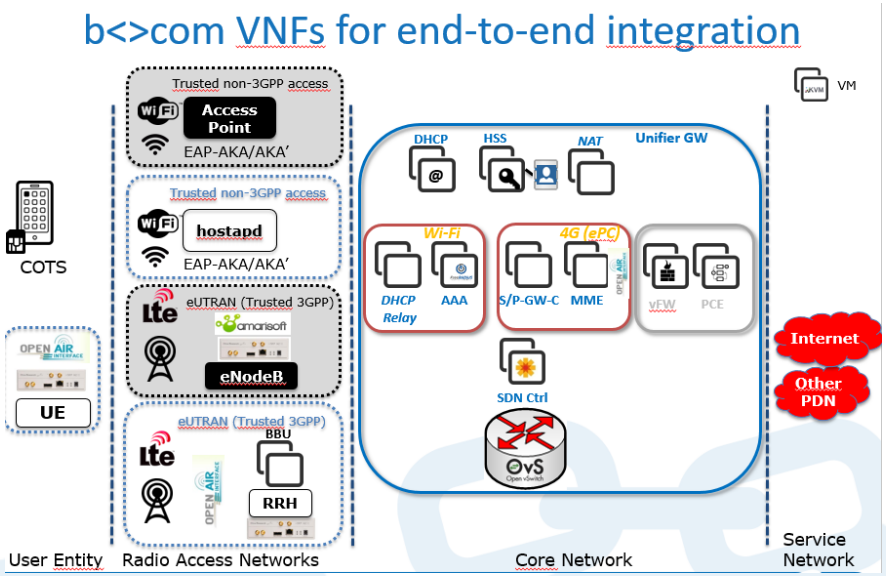
- **Product vision**
- **Technical roadmap** detailing features and their scheduling

5G Security enablers
Deliverables so far released

Security Enablers	R1	R2
Technical Roadmap	Deliverable D3.1 - 5G-PPP security enablers technical roadmap (early vision)	Deliverable D3.5: 5G PPP security enablers technical roadmap (Update)
Open Specifications	Deliverable D3.2 - 5G-PPP security enablers open specifications (v1.0)	Deliverable D3.6 - 5G PPP Security Enablers Open Specifications (v2.0)
Software Release	***Not public***	***Scheduled Aug'17***
Documentation	Deliverable D3.4 - 5G-PPP Security Enablers Documentation (v1.0)	

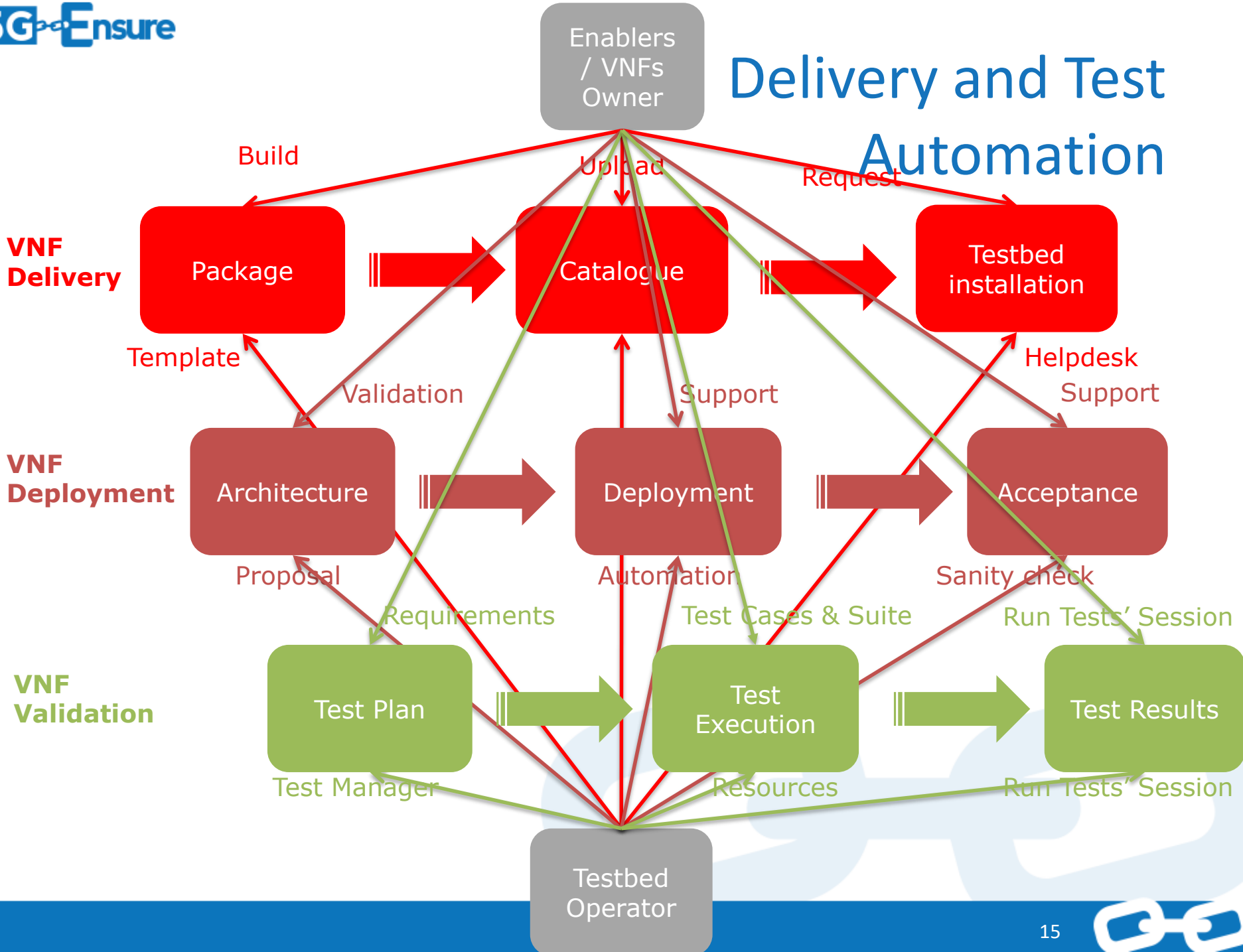
Testbed architecture





Full details: [Deliverable D4.1 - 5G Security testbed architecture]

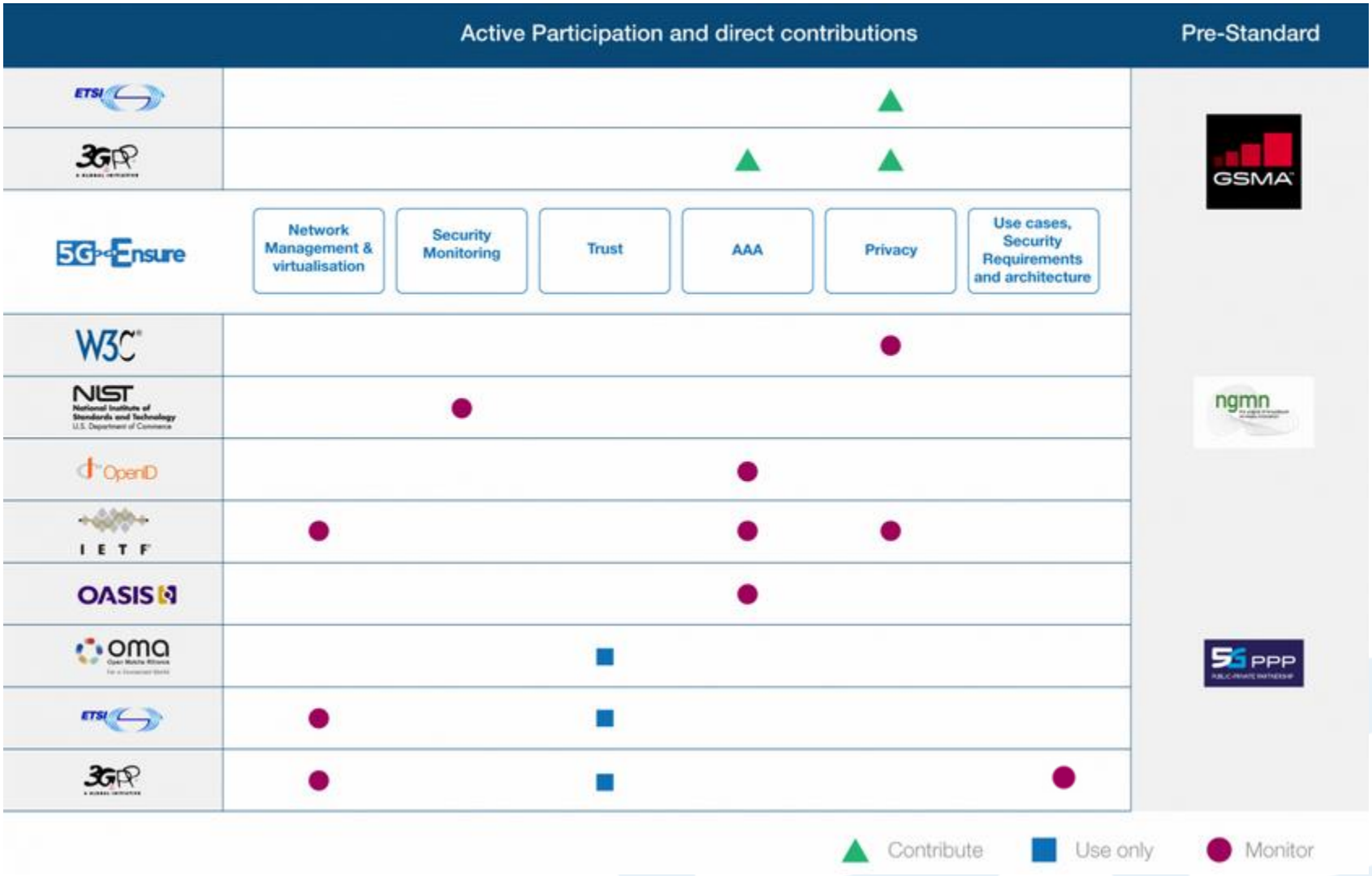
Delivery and Test Automation



5G-ENSURE KPIs

KPI		Comment
#Testbed Users	34	From 8 organisations
#Testbed nodes	3	b<>com, VTT, Nokia
#CPU Cores	80	Currently in use for 5G-ENSURE Out of an overall capacity of 512 CPU Cores
#VM Flavours	3	vSmall (1 CPU, 2 GB RAM, 20 GB HDD) vMedium (2 CPU, 4 GB RAM, 40 GB HDD) vLarge (4 CPU, 8 GB RAM, 80 GB HDD)
#Operating Systems	2	Ubuntu CentOS
#VM	25	
#Enablers	17	Available in catalogue
#Instantiated Enablers	16	Deployed on testbed
#Test plans	15	Filled in TestLink
#Validated Enablers	11	Test plan sucessfully passed

5G-ENSURE Standardisation Plan



5G PPP KPI (1/2)

- 5G ENSURE project goes towards the fulfillment of the 5G PPP KPIs which were selected as more relevant for the project

Performance KPIs		Project contribution	Progress	
P4	**Creating a secure reliable and dependable Internet with "zero perceived" downtime for services provision**	*Definition of 5G security* relevant *use cases*	- **31** *use cases* grouped in 11 security clusters	- 100%
		Security and privacy enablers in the main 5G security areas/domains	- **24 enablers (R1 & R2)** identified	- 100%
			- **17 enablers (R1)** specified and developed (**available since October 2016)**	- 100%
			- 7 enablers (R2) have also been specified (as new enablers and as additional features)	- 100%
			- 7 enablers (R2) are now under development (**available by August 2017**)	- 50%
		5G security architecture	- first design and initial mapping with the security enablers (R1) **available since November2016**	- 50%
		5G security testbed	- **available since August 2016**	
			- R1 enablers under integration and tested	- 89%

5G PPP KPI (2/2)

Societal KPIs		Project contribution	Progress	
S1	**Enabling advanced user controlled privacy**	*Definition of 5G privacy* relevant *use cases*	- **8** use cases concerning the user privacy	- 100%
		Privacy enablers	- **5** privacy enablers **(R1 & R2)** identified	- 100%
			- **2 enablers** (R1) specified and developed (**available since October 2016)**	- 100%
			- 3 additional enablers (R2) have also been specified (as new enablers as well as additional features)	- 100%
			- 3 additional enablers are under development (**available by August 2017**)	- 50%

- **Focus:** give users increased privacy by providing, both at the network and infrastructure level, and at service or application level, enhanced security mechanisms like confidentiality to subscriber and device identities

5G-ENSURE & Joint 5G PPP Activities

Mobile World Congress 2017 (MWC17) , **27 February 2017**

5G-PPP Cross-project workshop, 07 February 2017

The Second Global 5G event, Rome, 09-10 November 2016

5G-ENSURE showcases its outputs at exhibition stand during Global 5G this November.

EuCNC2016, Athens, 27-30 June 2016

5G-ENSURE presents its results. **First workshop of 5G-PPP Security WG lead by 5G-ENSURE**

Workshop on Security in Virtualised Networks , 10 June 2016

Co-chaired by 5G-Ensure

5G PPP projects @ETSI workshop: "5G, From Myth to Reality", 10-11 May 2016

5G-ENSURE is attending the 2-day ETSI Workshop in the context of the H2020 program of the European Commission

NetWorld2020, 19 April 2016

5G-ENSURE joins 8 other 5G-PPP projects at Networld2020 to discuss priority actions and future steps.

5G-ENSURE future events and demo

- 5G-ENSURE will mainly focus on demos of 5G Security enablers developed as per areas covered (i.e. IAM, Privacy, Trust, Security Monitoring , Network Mgt and virtualisation isolation).
- It will also demo the 5G security testbed and its potential combined with enablers catalog.

EUCNC 2017 June 12-15
European Conference on Networks and Communications | Oulu, Finland

[EuCNC Workshop on 5G Security]
[5G-ENSURE Demo Booth at EuCNC]

[2nd 5G-ENSURE Project Workshop]

- [NetFutures 2017, June 28-29]
- [5G-ENSURE & CHARISMA @2nd International Workshop on Security in NFV-SDN (SNS 2017), 3 July 2017]
- [5G PPP @ Helsinki 5G week, 18-21 September]

5G Ensure

5G Enablers for network and system security and resilience

5G-ENSURE: http://www.5gensure.eu

contact@5gensure.eu

@5GEnsure

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 – October 2017

The 5G Infrastructure Public Private Partnership (SG PPP)