The 5G Infrastructure Public-Private Partnership

5G-PPP Security WG

5G PPP Phase 1 Security Landscape Whitepaper overall presentation

ETSI CyberSecurity Week

16.06.2017

WG chairs: pascal.bisson@thalesgroup.com / jeanphilippe.wary@orange.com

5G-PPP Security WG

- **The purpose of the group is to:**
  - **Bring together the projects within the 5G-PPP that have common interest in** the development and progression of **5G security**.
  - **Ensure that the projects are working in a complementary manner towards coherent & consistent goals**, exchanging ideas, minimizing the duplication of effort, contributing towards relevant standards
  - **Cooperate on the development of compatible components, demonstrators, promote exchange of data and results *within the WG and across WGs***.

5G Infrastructure PPP
The European path towards global next generation communication networks

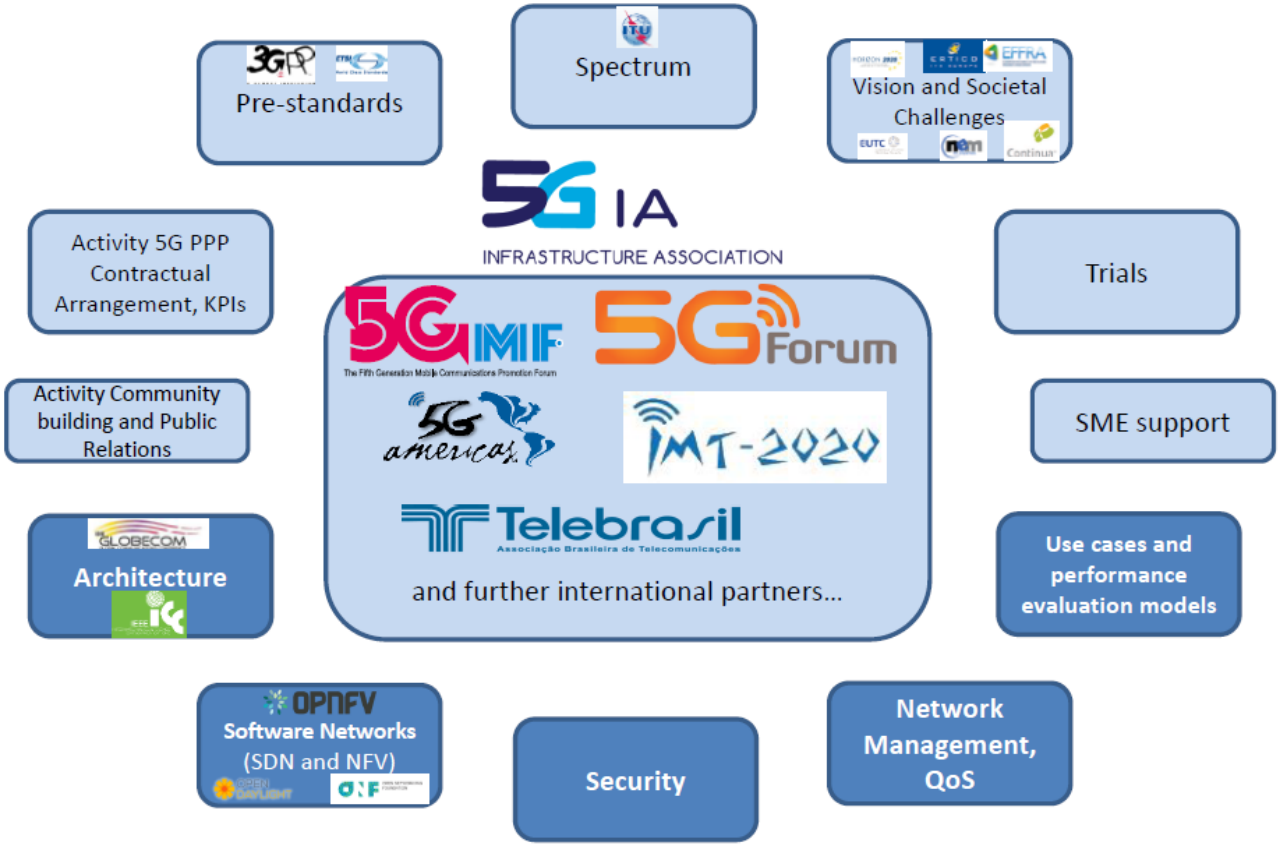
5G-PPP Security WG

- 5G-PPP Security WG is open to all interested projects.
  - Constituency from Phase 1 :

- New projects Phase II interested would be on-boarded

5G Infrastructure PPP
The European path towards global next generation communication networks

5G-PPP ecosystem



A rich ecosystem for Security WG to liaise and contribute …

5G-PPP Phase 1 Security Landscape

5G-PPP Phase 1 Security Landscape

- New 5G major security requirements and risks
- Security Architecture
- Access Control to 5G
- Privacy
- Trust models
- Security monitoring & management
- Slicing / Virtualisation and Strong Isolation
- Security standardization
- 5G open security challenges

5G Infrastructure PPP
The European path towards global next generation communication networks

5G Infrastructure PPP
The European path towards global next generation communication networks

New 5G major security requirements and risks

5G major Security Risks

- Unauthorized access or usage of assets
- Weak slices isolation and connectivity
- Traffic embezzlement due to recursive/additive virtualization
- Insufficient technology level readiness
- Difficulties to manage vertical SLA and regulation compliance
- Slicing vs Neutrality
- Trust Management Complexity

5G Security Requirements

- **5G Security & Privacy** level higher or equal to 4G level
- Security Automation across multiples domains
- Security Monitoring (coordination between multiple domains and systems)
- Security Management
- Security Trust → Liability Schemes between parties
- Inter-tenant/Slice Isolation (from E2E perspective)
- 5G Regulation Conformity (Neutrality, Data Retention, GDPR, e-Privacy, critical operators, new telecom regulation…)

Challenges

- As stated in the whitepaper, the listed 5G security requirements and risks are not complete and also 5G-PPP phase 1 project oriented.
  - Improve, contextualize, and expand for the next steps…
- Include security requirements and risks input from 5G-PPP phase 2 project in a structured manner.
  - Provide a template or guidelines in the beginning to all the projects.
- 5G security requirements and risks to cover all Verticals aspects of 5G security in different contexts.

Security architecture for 5G

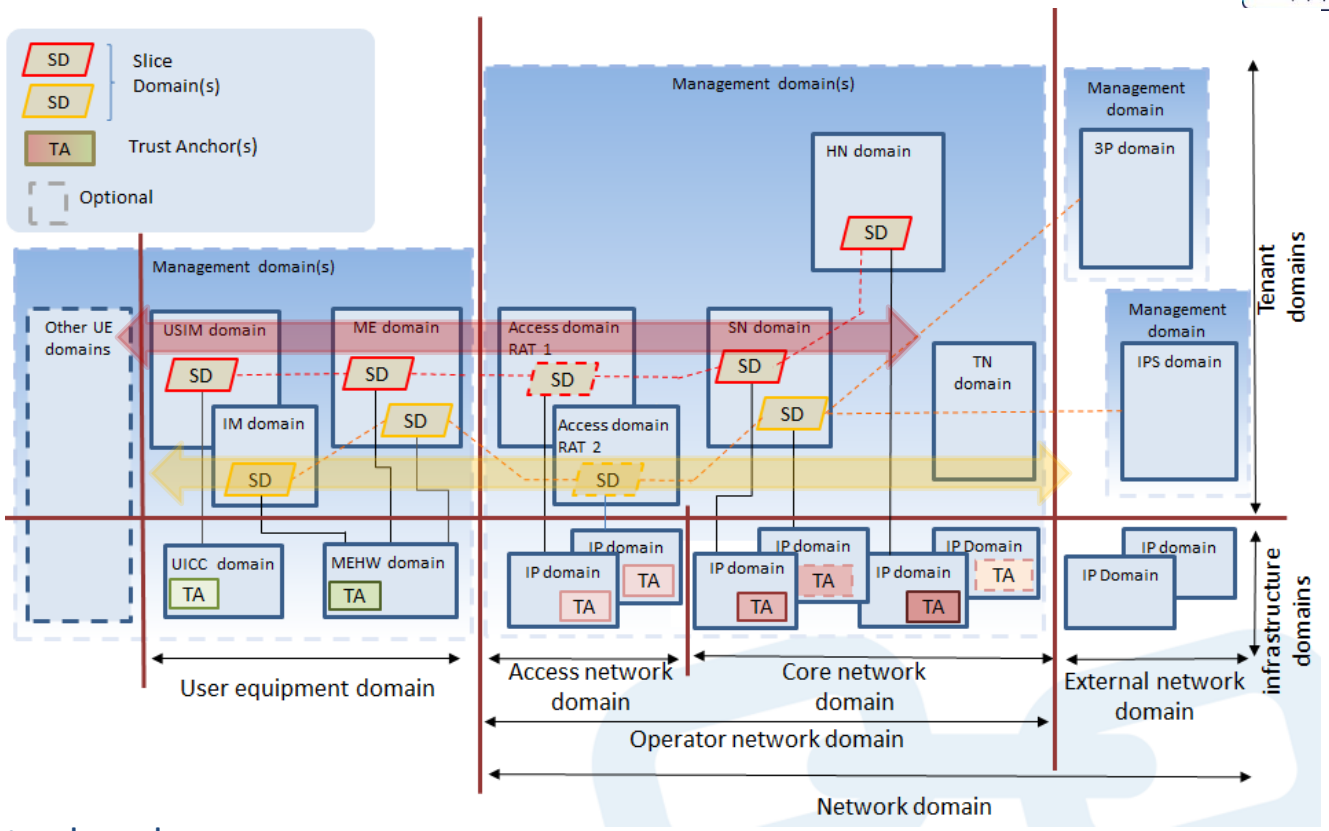
Security architecture for 5G

- Why a new security architecture ?
  - wider scope
  - no explicit and complete trust model documented for 3G and 4G networks,
  - virtualization and management left out of scope which is not sustainable in 5G
  - for mission critical services a completely new threat and risk situation occurs

- In the meantime not reinvent the wheel …

5G (Security) Domains

UICC Domains
MEHW : Mobile Equipment Hardware
IP: Infrastructure Provider
ME: Mobile Equipment
USIM Domains
IM: Identity Management
SN: Serving Network
HN: Home Network
TN: Transport Network
3P: 3rd Party
IPS: Internet Protocol Service



Changes introduced:

- distinction between the set of physical domains which we call Infrastructure Provider Domains (IP Domains) and the logical/functional domains which we call Tenant Domains,
- slices (that may extend across both access and core domain) which form a kind of transversal “domains-across-domains” are model by special Slice Domains,
- define special Management Domains for management functionality
- (Additional) UE Domain added to capture the so called direct-mode, UE-to-UE communication

Challenges

- Further develop 5G Security Architecture
  - Work on-going (next revision planned by of Oct'17)
    - Specific actions conducted to better materialize risks captured and security controls to address them,
- Integration within overall 5G Architecture
  - At stake here embodiment of 5G Security Architecture with overall architecture
    - Work engaged here with the following 5G WGs : Architecture, NetMgmt & QoS , and SDN/NVF (Virtualization) (see https://5g-ppp.eu/5g-ppp-work-groups/)
- Continuously benchmark 5G Security Architecture through successive releases to get feedback and integrate
  - Overall objective to get it shared by the 5G PPP Community and beyond

5G Access Control

5G Access Control

Until 4G, the mobile network access control (AAA) is homogeneous, secure, and interoperable worldwide over visited network infrastructures.

Forecast 2020 :

- anticipated 5G uses cases : more than 25 billion of device
- The signalization amount increase is one of the **major bottlenecks** for the 5G development as a low delay and reliable network for IoT devices.

Access Control open points

Vertical Services should be aware of devices/customers security context and access security levels

- Propagation of collected user equipment security level or stakeholders' trustworthiness evidences from the access control (performed at the edge of the 5G network) to the vertical services (operated in some slice).

already anticipated in 5G-PPP Phase 1 projects

Access Control open points

Potential heterogeneity of access control security levels.

- A multi-tenant 5G infrastructure could be composed of many different types of slices i.e. RAN slice, Vertical slice, Core slice. Indeed, the security level for authentication may vary between slices.
- 5G MUST HAVE **an high level of isolation between slices** within the multi-tenant 5G Infrastructure.


5G Infrastructure PPP
The European path towards global next generation communication networks

Privacy

The way forward

- **Privacy-by-design** to be applied in each 5G area
- Privacy Regulation (for instance : GDPR for Europe, e-Privacy, new Telecom regulation)
- For subscribers and 5G privacy enablers that aim to enhance user data protection at several layers (i.e. network, application) and put him/her in control
  - Still challenging: scalability and adaptability of solutions to IoT context (also constraints) , abundance of verticals (and value add services) that makes difficult creation of a standard user privacy policy specification language
- *For service providers: homomorphic encryption seems to be a fitting solution*
  - Still challenging: overcome its limitations (slow and resource consuming).

Trust models

The way forward

- Defining Trust Models applicable for 5G
- Quantifying the trust referents from the 5G system
- Enforce the adequate stakeholder behavior requirement into the service-level-agreement (SLA) of 5G.
- Evolution from **Trust** concepts to **Liabilities** concepts between actors of the 5G ecosystem.

Security monitoring & management

Security Monitoring in 5G Networks

- The 5G threat landscape needs to be captured and continuously monitored
- Novel concepts (e.g., SDN and NFV) applied to critical infrastructures requires investigation for new potential security risks
- But, how? Some first answers are:
  - **Identification** of different **security threats** associated to several typical 5G use cases and scenarios
  - **Analytics** applied to security operations management in a 5G context
  - Deployment of **security configurations** which are **dedicated for particular applications or users** ➔ isolating application specific connections

Security Management in a Common Logical/Virtual Layer: Approaches

- **Mechanisms for fast signature** matching and fast processing at data plane
- Different mechanisms will be necessary to **secure the control plane in 5G**
  - Control the access to network resources and enforce access control policies
- **Coordination of security functions** distributed across various VNF-Components
  - Typical security service in 5G networks: **composition of multiple, differentiated and specialized security Network Functions (PNF and VNF)** chained into an end-to-end service flow
- **Run-time network adaptation mechanisms** for incident response and mitigation applied to 5G components
  - Decision making, changing rules or user privileges, correcting system problems, etc.
- Policy-based security management
  - Virtualization of resources + security requirements at different levels or domains

Security Management in a Multi-layer Security Management: Approaches

- **Situational awareness** for 5G security management
  - Tendency: more **cognitive methodologies** facilitating understanding the environment through **contextual** analysis
- **Mixed integration of virtualized and physical security gateways/functions**
  - Hybrid network architectures in which PNFs and VNFs for security gateways/functions co-existing
- **Isolation vertical**
  - Ensuring secure **multi-tenant support** across 5G infrastructures that rely on SDN and NFV practices to automate the deployment of services and functionalities

Some Key Research Challenges

- How to **combine** the needs for **end to end security monitoring** with the request of **strong isolation** between slices
- How to **adapt in real time an end to end security monitoring system**
- Infrastructure sharing by multiple virtual network operators will require **strict isolation at multiple levels** in order to ensure absolute security
- The use of SDN in cross-domain setups and the absence of multi-operator collaborative incident detection mechanisms introduce **new threats**

5G Infrastructure PPP
The European path towards global next generation communication networks

Slicing / Virtualisation & Strong Isolation

Introduction

- **Logical instantiation of a network**
  - With all the functions and settings that the network needs to operate, in the context of specific use case or business model.
- **A single, common physical network is separated into multiple complete, virtual, end-to-end (E2E) networks.**
- To guarantee, for each network slice:
  - minimum of Resources (e.g. computing resources),
  - QoS parameters (e.g. low latency) and
  - Services (e.g. security or traffic shaping services),
- **Networks customized & optimized for different use cases/business models/market scenarios.**

Open Issues

- **Isolation guarantees** between slices and used network services
  - Deliver and maintain a continuous chain of isolation evidence (from user or operator perspective) with respect to local regulation
- **Multi-level isolation**, for secure infrastructure sharing by multiple virtual network operators.
  - Control-plane, data-plane and resource isolation must be ensured to achieve **zero correlation** among different tenants' operations.
- **Monitoring of network activities across different domains** (inter-domain flow assignments, isolation, conflict resolution), also with respect to cross-country regulation
- **Slicing vs. Net Neutrality**
- For true end-to-end slicing **user equipment,** along its intricacies (e.g. lack of total control) will have to be included in the slicing

5G Infrastructure PPP
The European path towards global next generation communication networks

Security standardization

Standard: Main security topics

the main security topics, on which we have been active so far, where the 5G-PPP Security WG will encourage co-signed contributions to be elaborated by the H2020 projects are the following:

- **Security Architecture**
  - Security architecture aspects have mainly concerned design choices (e.g. where to place termination points for user plane ciphering)
- **AAA**
  - AAA services are central in the scope of 5G security, at least to protect frequency and radio/communication resources, to deliver 5G networks services on demand and to comply with different regulation constraints
- **Privacy**
  - In particular subscription privacy is a very important area for Next Generation system
- **Network Slicing Security**
  - The support of network slicing has been identified as a key issue to meet diverse use cases (e.g. Internet of things, Enhanced broadband, critical communication) on top of the same 5G network.

http://5g-ppp.eu

Thank you for your attention!