Workshop on Accountability and Liability for 5G and beyond – WAL5Gplus
16 June @ 9:00 am - 5:30 pm

INSPIRE-5Gplus

Intelligent Security and Pervasive Trust for 5G and Beyond

Jean-Philippe Wary, Orange

www.inspire-5gplus.eu

5G Security Risks to be Tackled

▸ **Unauthorized access** or usage of assets

▸ **Weak slices isolation** and connectivity

▸ **Traffic embezzlement** due to recursive/additive virtualization

▸ **Difficulties to manage** vertical SLA and regulation compliance

▸ **Trust management insufficient** for 5G infrastructure complexity

Major Goals of INSPIRE-5Gplus

- **Ensure conformance of security level** to legislative and standards requirements
- **Provide a dynamic security framework** embracing the end-to-end 5G network-service chain

A smart, trustworthy and liability-aware 5G security platform for future connected systems

Novel Security Architecture for 5G
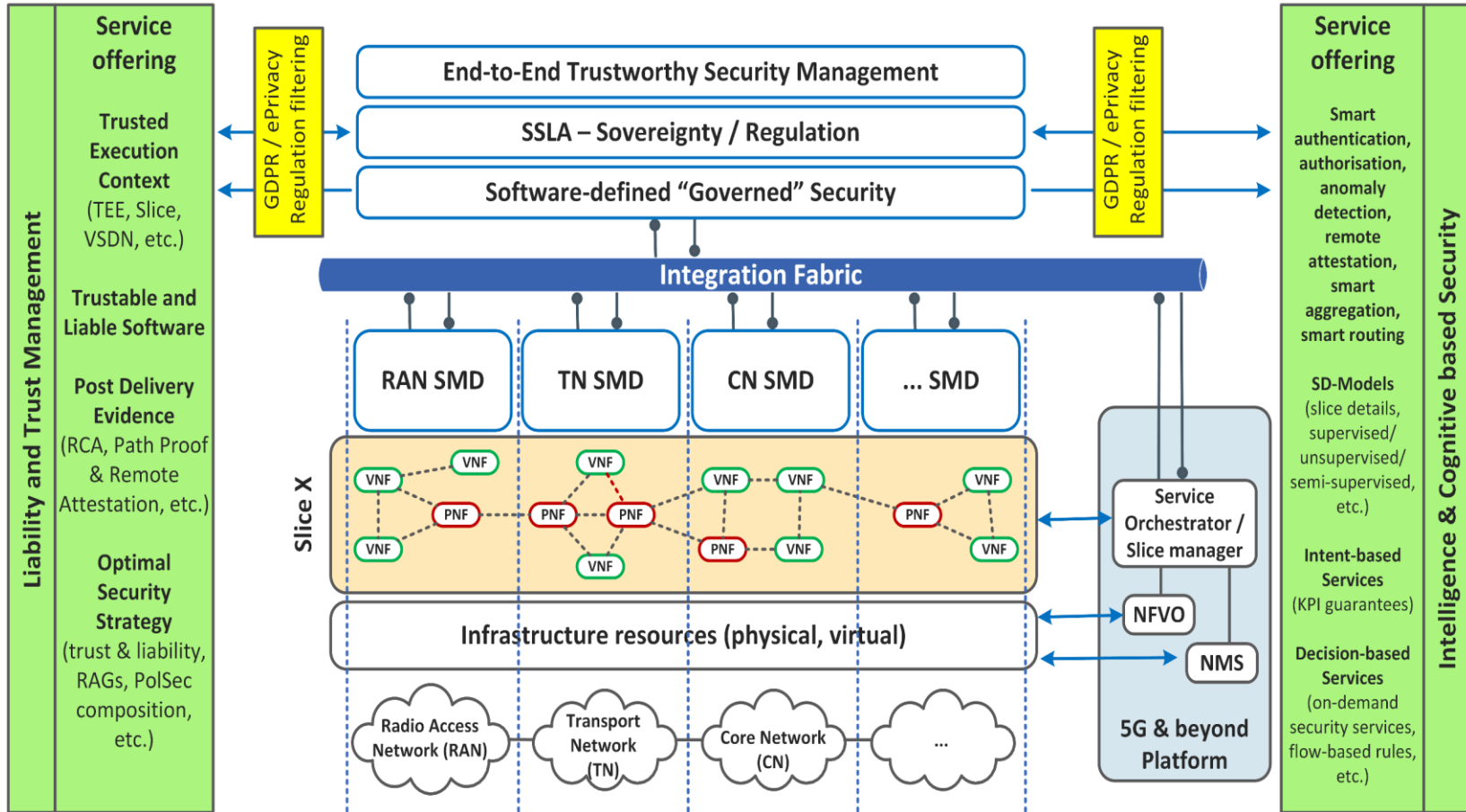
INSPIRE-5Gplus

Main Results Envisaged by INSPIRE-5Gplus

- **Comprehensive report** on current 5G security landscape
- Intelligent and autonomic end-to-end **cyber security services** for detecting and mitigating threats in 5G networks
- Evolved and new **5G security assets- technologies**
- Novel **integration and experimentation framework** for validating specific 5G security use cases in INSPIRE-5Gplus

INSPIRE-5Gplus at a Glance

Research Programme

Horizon 2020 / 5G PPP

ICT-20-2019-2020

Duration

36 months / Nov 2019 – Oct 2022

Total Budget

5.99 million euro

Project Coordinator

Eurescom, Germany

Technical Manager

Thales, France

Liability questions for INSPIRE5GPlus

INSPIRE-5Gplus

Trusted Operator

- Common Criteria certification of equipment (EAL4+)
- SLA for QoS (easy to measure)
- Usage of TEE, HSM, USIM
- E2e authentication / ciphering
- Secure component (HW / SW)

No real security commitment

Liability questions for INSPIRE5GPlus

Trusted Operator ➡ 'Trustable' Operator

Trusted Operator

- Common Criteria certification of equipment (EAL4+)
- SLA for QoS (easy to measure)
- Usage of TEE, HSM, USIM
- E2e authentication / ciphering
- Secure component (HW / SW)

No real security commitment

'Trustable' Operator

- Security SLA = contract ?
- Measurable security KPIs = penalties ?
- Which component is in charge of which SLA / KPIs = orchestration (over multi domains) ?
- RCA, which component originates the flaw / incident ▯ is responsible for a failure or bad KPIs = proof convention or more ?
- Remote attestation / Path Proof (crypto, protocol, proof) – contextualization of services = sovereignty ?
- Multiple Certification schemes Composition = which models ?
- Transparency, simplicity and fairness of dynamical contractualization

www.inspire-5gplus.eu

Further Information

Website: www.inspire-5gplus.eu

Twitter: @INSPIRE_5Gplus