5G Cybersecurity

Initiatives and challenges

Patricia Diez

Antonio Pastor

Patricia Diez, Antonio Pastor
Telefónica.
21.04.2021

Who we are?

Telefonica experts

We are 2 experts in security in Telefonica. Focuses on different areas and activities. For short to long-term technologies

Patricia Diez

Patricia Díez Muñoz has worked in the Telecommunications sector for more than 20 years and in the Telco security sector, at Telefónica, as the global responsible for network, IT platforms and client devices, security within CTIO area, for 10. Its main tasks include the development of security guides for the deployment of fixed and mobile networks, security tests on implementations, participation in the different standardization bodies, performance of security tests on deployments, security of the services offered to our clients, support to the rest of global areas both internal and business, development of regulations and security requirements for the different manufacturers of mandatory compliance

linkedin.com/in/patriciadiez

Antonio Pastor

Antonio Pastor received the M.Sc. degree in industrial engineering from UC3M in 1999. Since then, he works on engineering different worldwide units in Telefónica. Now, in CTIO, he is involved in network security innovation activities, including virtualization, SDN, and ML

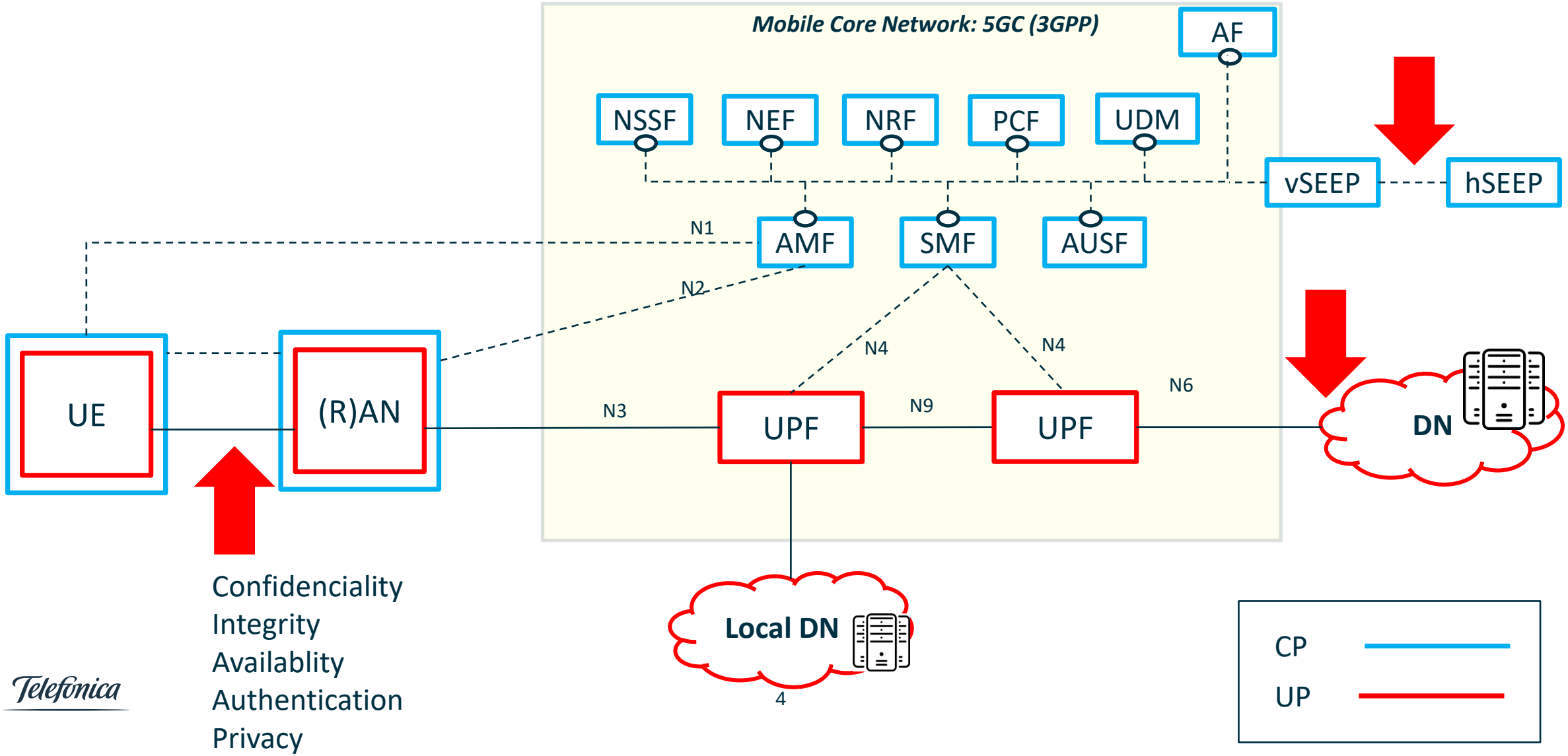
linkedin.com/in/a2pastor

PUBLIC USE

Introduction to 5G security

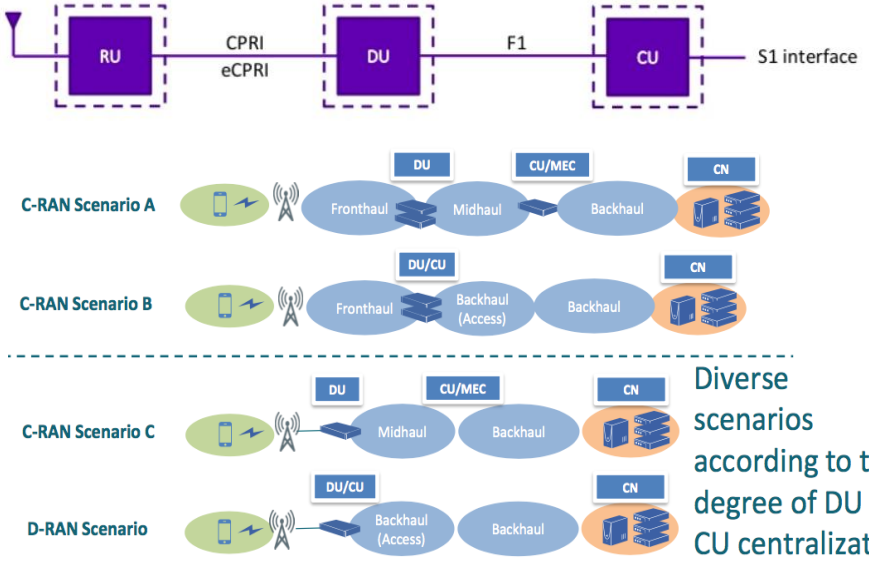
5G general vision

What people usually see in terms of 5G security



5G multidomain vision

What Operators usually see

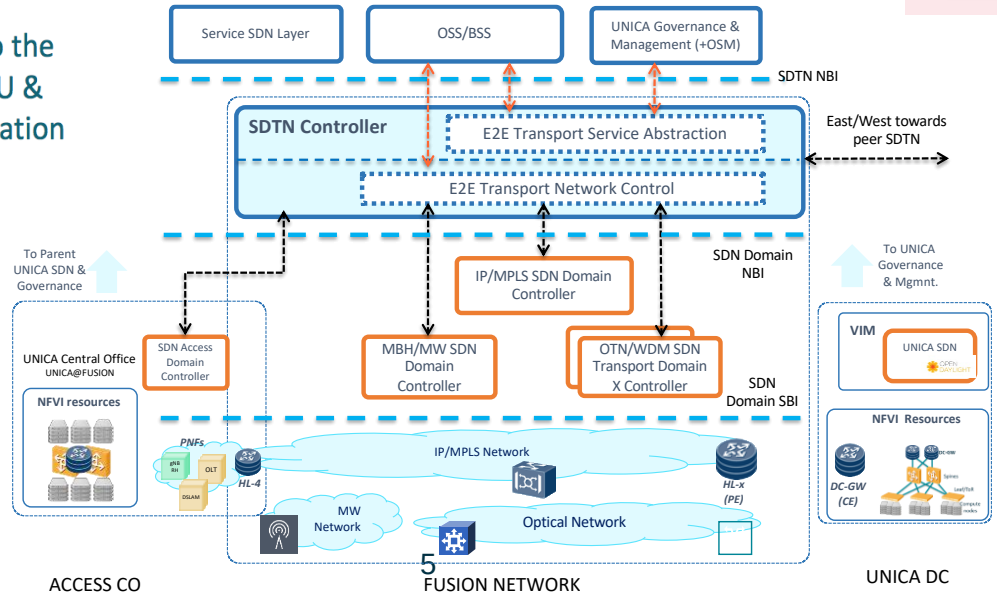


Diverse scenarios according to the degree of DU & CU centralization

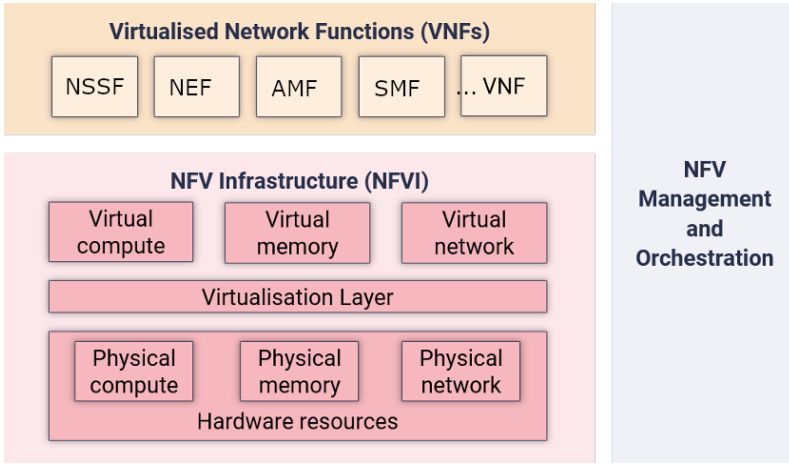
Radio Access

- **5G distributed model**
  - Multi-haul (front, mid, back) model
  - Transport
  - Ege/Cloud/NFV
- **Management frameworks**
- **Protocols**

Transport



Cloud Telco



PUBLIC USE

Risks related to 5G

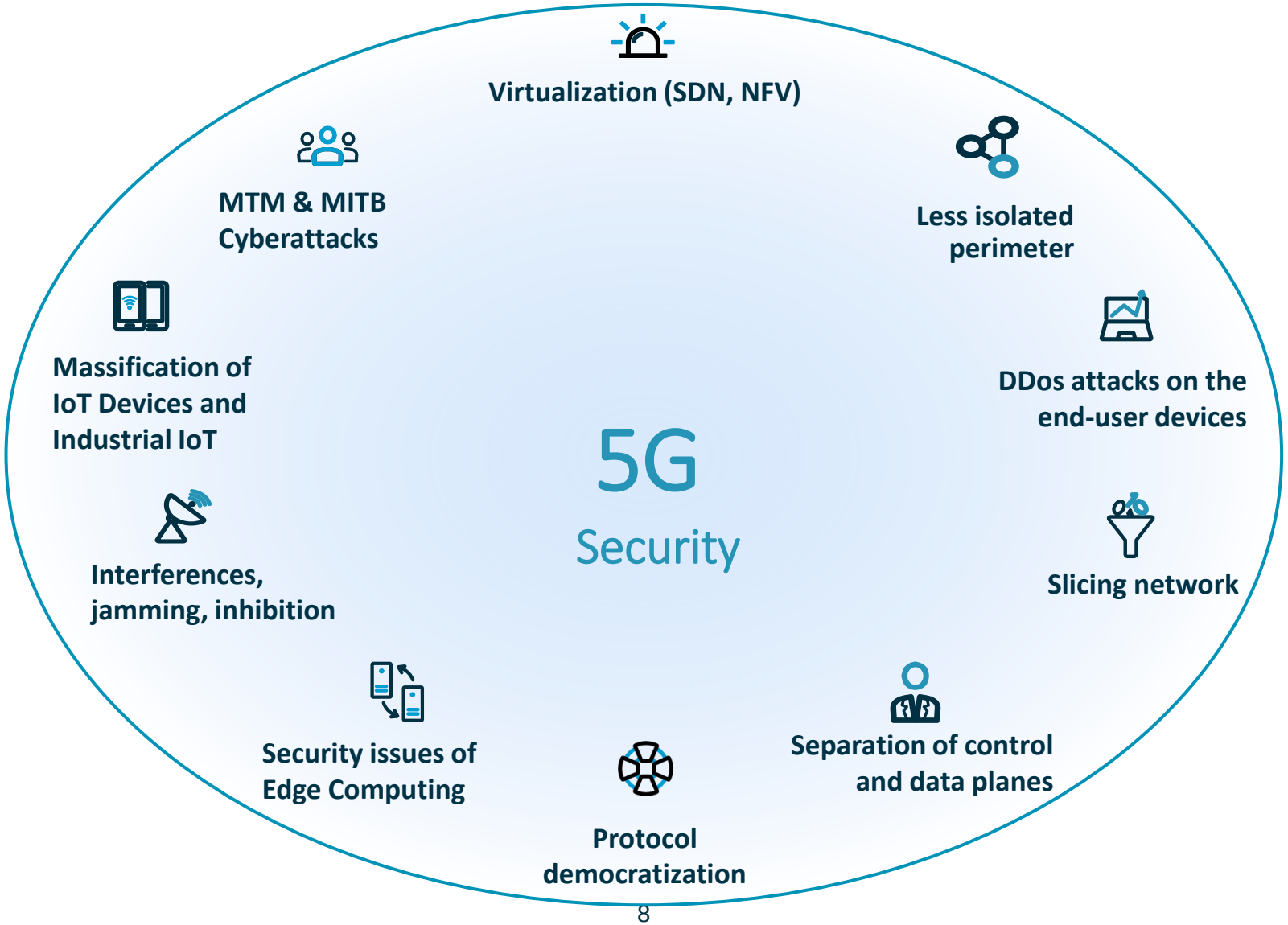
Risks related to 5G

Tomorrow's security must **support elastic, edge-to-edge, multi-stakeholders strategies** to address new challenges

Security risks to take into consideration in 5G deployments

- User Equipment (UE)
- Radio Access Network (RAN)
- Edge deployments and MEC
- Signaling
- Network Slicing
- Virtual environment (SDN/NFV)
- Core SBA
- IT protocol
- Operational
- Open Source usage
- One compact equipment -> different layers
- Others not security specific

Risks related to 5G



PUBLIC USE

Security controls in 5G

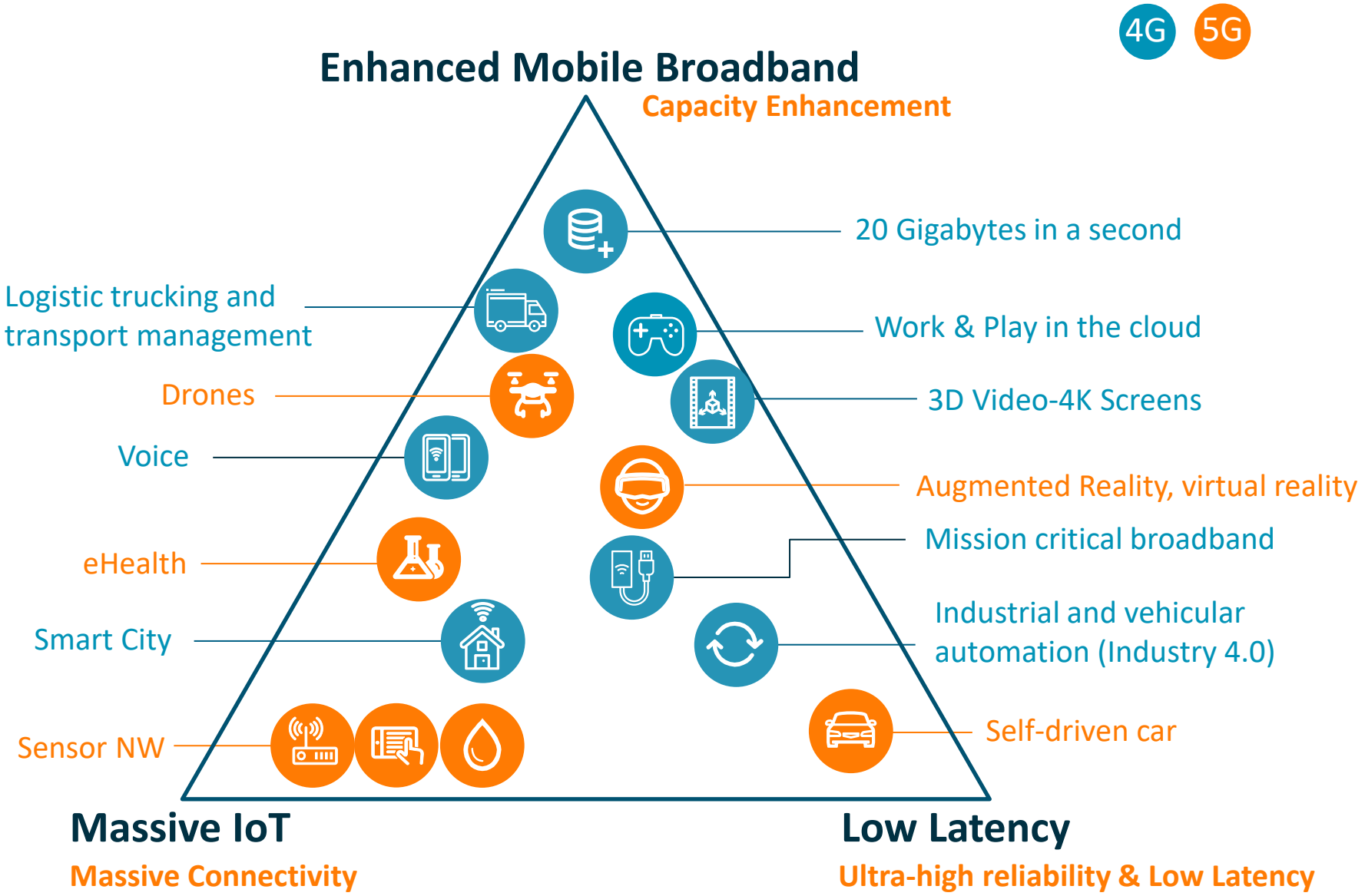
Security controls in 5G

Controls

- Security **Policies**: privacy and cybersecurity governance
- Security **life-cycle**
- New Security **standards and certifications**
- Knowing who is in your **supply chain**
- Adopt a **Zero-Trust strategy**

5G New use cases

5G New use cases



PUBLIC USE

Opportunities of 5G in cybersecurity

Opportunities of 5G in cybersecurity

Telcos have a responsibility to create secure networks, and secure connectivity

New 5G networks
secured by design

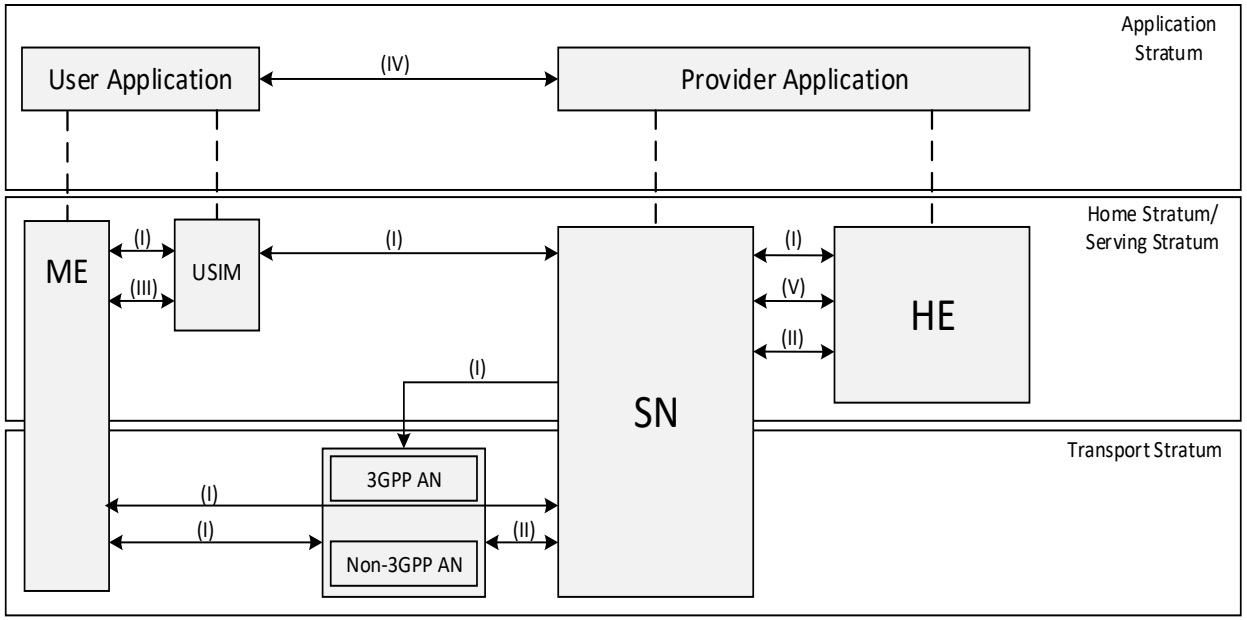
- **Proactive** and **multilayer approach**
- Reduce the risk though **Zero Trust networks**.
- The applications will be hosted at the edge.
- Machine learning and artificial intelligence

PUBLIC USE

3GPP Standardization body introduction

3GPP Standardization body introduction

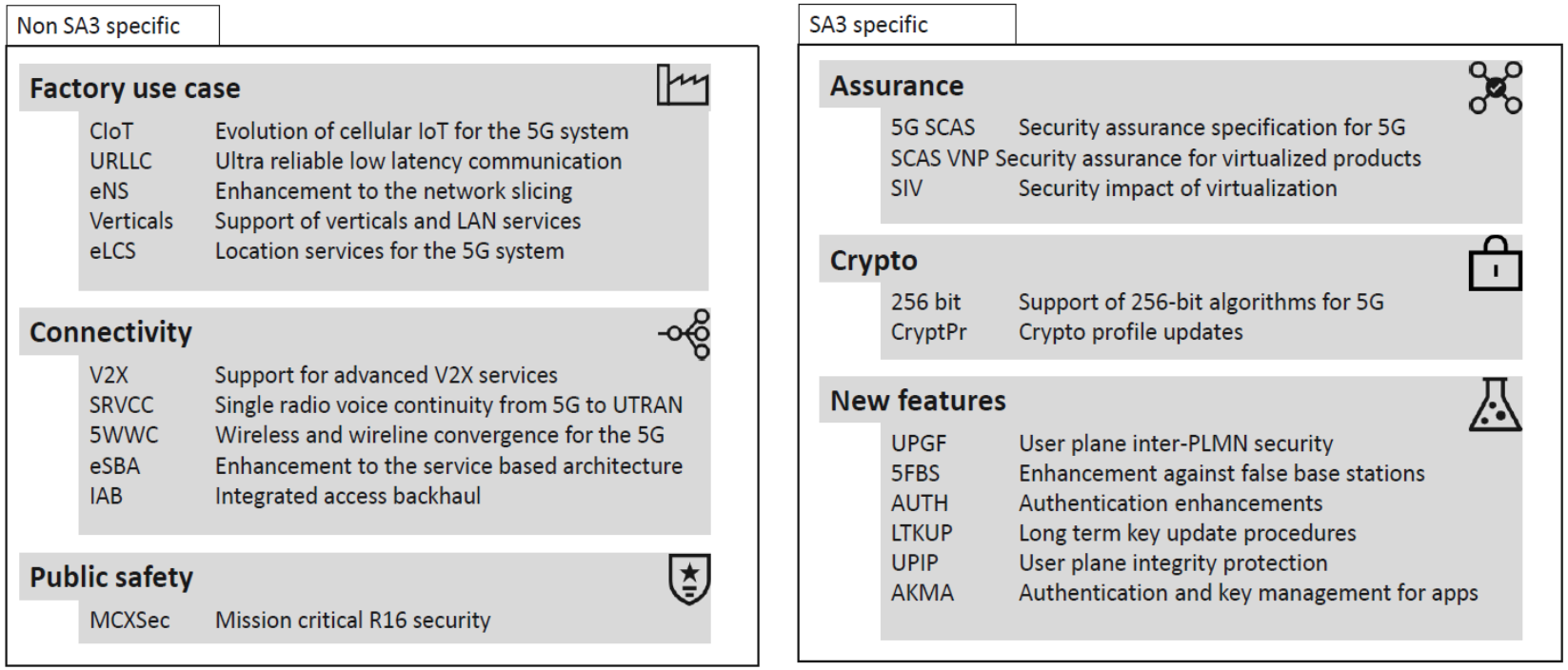
Security Domains defined by 3GPP



- Network access security (I)
- Network domain security (II)
- User domain security (III)
- Application domain security (IV)
- SBA domain security (V)

3GPP Standardization body introduction

3GPP overview



3GPP Standardization body introduction

Structure for Security topics on 3GPP sec archit document TS 33.501

1. Overview of security architecture
2. Security requirements and features
3. Security procedures between UE and 5G network functions
4. Security for non-3GPP access to the 5G core network
5. Security of interworking
6. Security procedures for non-service-based interfaces
7. Security aspects of IMS emergency session handling
8. Security procedures between UE and external data networks via the 5G Network
9. Security aspects of Network Exposure Function (NEF)
10. Service Based Interfaces (SBI)
11. Security related services
12. Management security for network slices

Annex A (normative): Key derivation functions

Annex B (informative): Using additional EAP methods for primary authentication (TLS)

Annex C (normative): Protection schemes for concealing the subscription permanent identifier

Annex D (normative): Algorithms for ciphering and integrity protection

Annex E (informative): UE-assisted network-based detection of false base station

Annex F (normative): 3GPP 5G profile for EAP-AKA'

Annex G (informative): Application layer security on the N32 interface

3GPP Standardization body introduction

Most relevant 3GPP specs talking about security

Spec	Title
TS 33.501	Security architecture and procedures for 5G System
TS 33.511	5G Security Assurance Specification (SCAS); NR Node B (gNB)
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS); Session Management Function (SMF)
TS 33.516	5G Security Assurance Specification (SCAS); Authentication Server Function (AUSF)
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TR 33.811	Study on security aspects of 5G network slicing management
TR 33.813	Study on security aspects of network slicing enhancement
TR 33.818	Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products
TR 33.835	Study on authentication and key management for applications based on 3GPP credential in 5G
TR 33.535	Authentication and key management for applications based on 3GPP credentials in 5G (AKMA)

All 3GPP specs can be downloaded from: https://www.3gpp.orgDynaReport/<spec#>.htm

PUBLIC USE

Improving 5G Security through GSMA CVD Programme

Improving 5G security through GSMA CVD Programme

Disclosures must describe new work and vulnerabilities that were **not previously in the public domain**

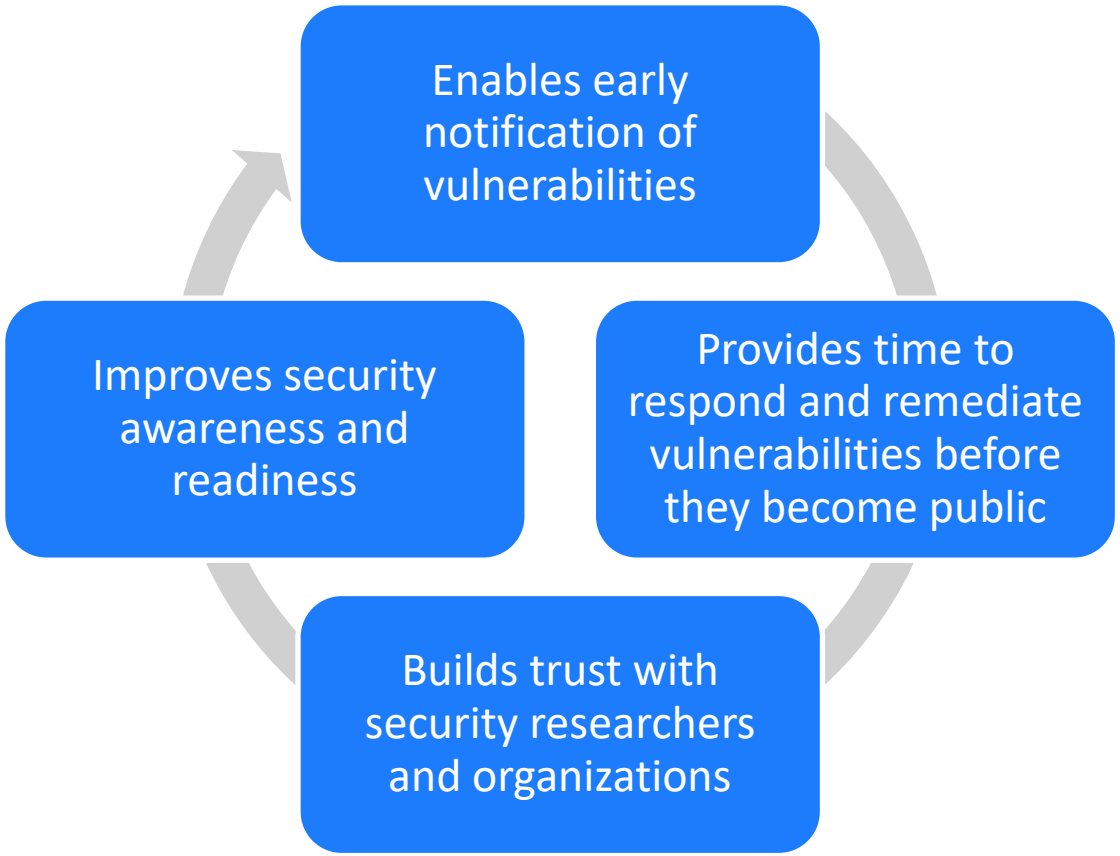
The identified security vulnerability must **not only apply to vendor specific technologies or services**

Must focus **on open standards based technologies** that are used across, or have significant impact on, the mobile industry.

Examples: 4G, 5G SIM toolkit, SS7, eSIM, AKA protocols, SIM box

Improving 5G security through GSMA CVD Programme

CVD Programme Beneficts



Improving 5G security through GSMA CVD Programme

- GSMA CVD: 5G research overview

- 14 pieces of research relating to 5G since 2017 (total 33)
  - Majority of these (86%) from Academic Researchers
  - Main issue: False Base Station, unprotected connection/paging

- Sometimes research identifies either:
  i. a known limitation of the 3GPP standard (i.e. not designed to protect) or
  ii. misconfiguration by vendor/operator

- Impacts include UE DoS, UE impersonation, spoofing, coarse-grain UE location, providing capabilities of a UE to the attacker, paging UE

More information:
https://www.gsma.com/cvd
If you are a GSMA member: IC2 group – search “CVD”

PUBLIC USE

Research view 5G Cybersecurity

Security topics in 5G and beyond

Security topic	Reuse from 4G (Work well) or new in 5G	Beyond 5G expectation (to improve)
Identity Management and provisioning	(U)SIM-based identity management & UICC & eUICC	Support diversified (unified) identity management mechanism Fake base station identity
Authentication and security termination	5G-AKA. EAP-AKA in Home only network Flexibility in security termination, multiple authentication (AAA)	New authentication demands (Slice, IoT, private 5G) IoT security (V2X, I4.0)
Network element security	4G network elements security (eNB to gNB)	Expand in NFV, cloud scenarios, TEE
Data protection algorithm	4G in use (AES, ZUC, public-key algorithms)	Post-Quantum computing (QKD, PQC), pervasive E2E encryption
Network Domain Security	Backhaul and IPsec	Multi-haul (CU/DU), E2E Security, SBA security (TLS), Network Slicing,
Privacy	Temporal identities concept Improve IMSI protection in initial auth (SUCI)	Pervasive encryption, trust measurement on networks (Cloud, slices, SDN)
Security Management and control	Based on legacy management solutions (OSS, EM) and technologies (SIEM, FW, IDS,etc..)	Complex networks require new solution: AI/ML, Close-loop Management, Data management

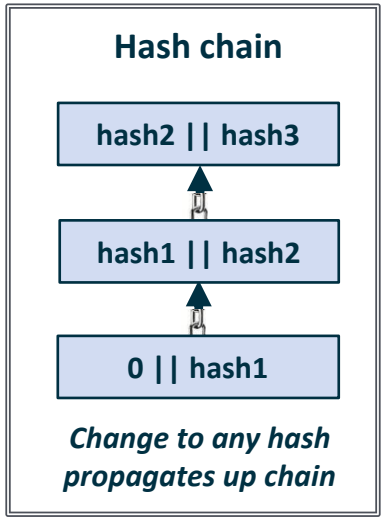
PUBLIC USE

Network element Security Focus in NFV

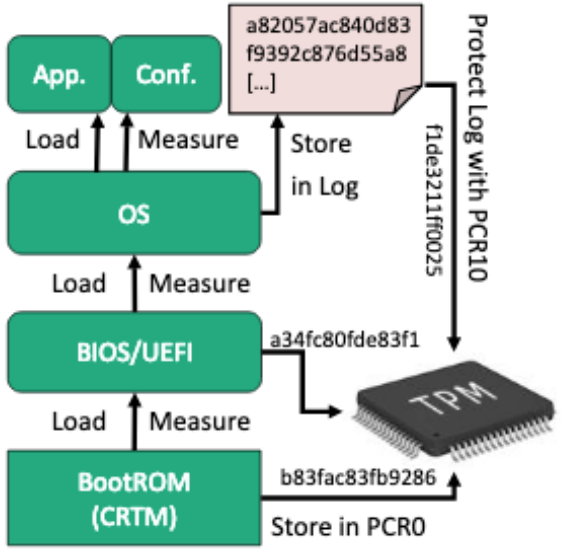
NFV: Remote Attestation

Integrity and verification of the cloudified 5G network functions (a.ka. Dockers*) components during their whole life cycle

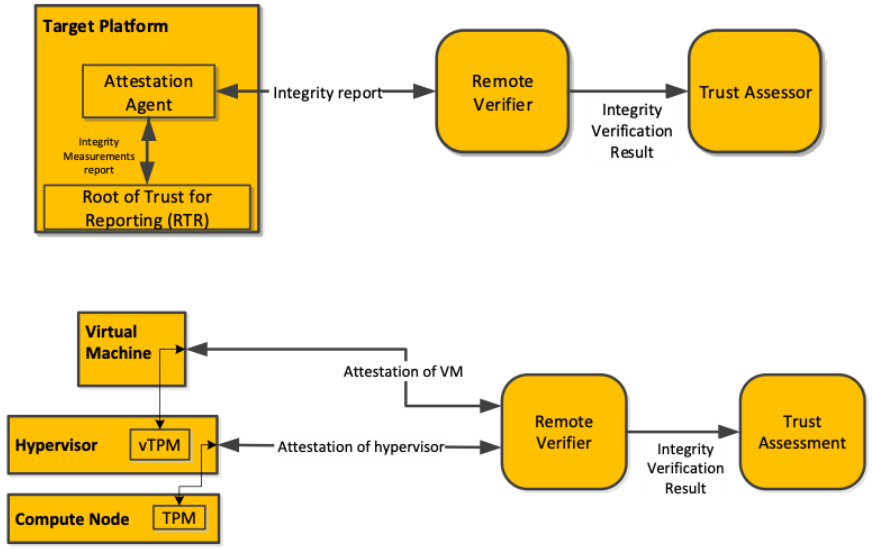
- Security chip/co-processor widely deployed.
  - Shielded execution of standardized commands.
  - Private keys never leave the chip (configurable).
- Enabler for high-level security features:



Measured boot



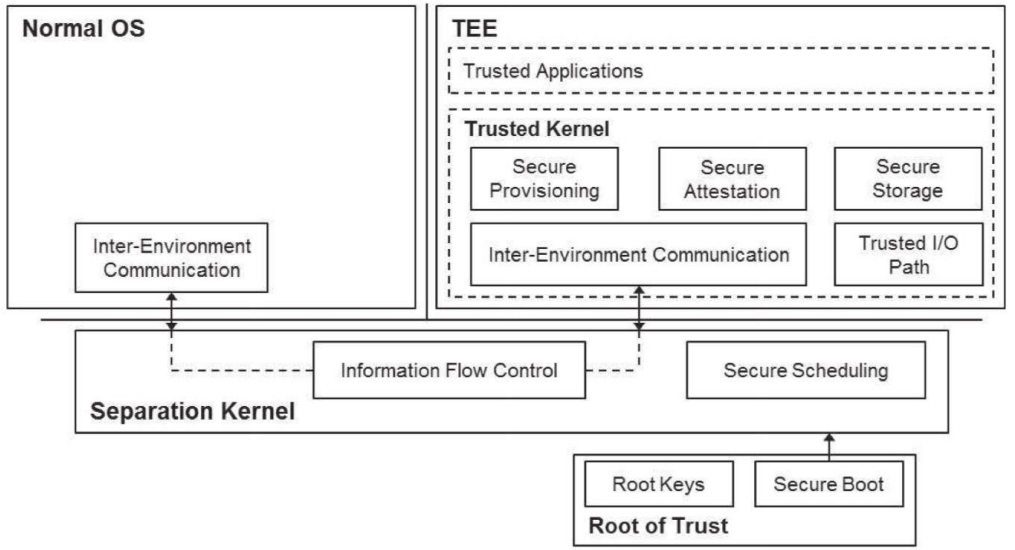
Remote Attestation



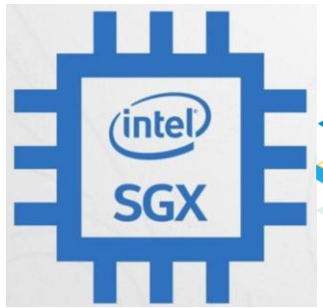
*Marco De Benedictis, & Antonio Lioy. (2019). Integrity verification of Docker containers for a lightweight cloud environment. Future Generation Computer Systems, 97, 236–246. http://doi.org/10.5281/zenodo.3267028

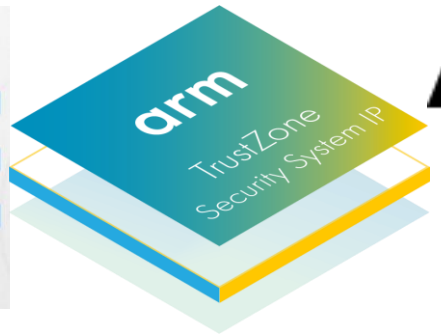
NFV: Trust Execution Environment

- Protect software integrity
- TEE Properties:
  - Memory Isolation
  - Code confidentiality/integrity
  - Data confidentiality/integrity
  - Remote attestation of Trusted Computing Base (the software that integrates a TEE)
  - Secure provisioning of Hardware TEE
  - Secure data sealing-storage



M. Sabt, M.Achemlal, "Trusted Execution Environment: What It is, What It is Not ", 14th IEEE International Conference on Trust, Security and Privacy In Computing Communications, Aug 2015, Helsinki, Finland.





PUBLIC USE

Data protection algorithm:

PostQuantum Era

Quantum Cryptography fields

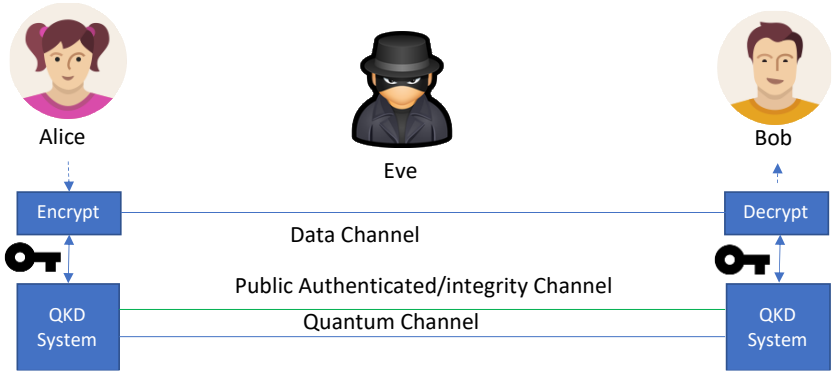
Main Technologies

Quantum Crytography are a set of technologies that leverage **the laws of quantum physics** to protect data, creating, in theory, totally secure communication channels.

QKD

Quantum Key Distribution technology sends **classical bits** though the network that are **encrypted using keys obtained with quantum technologies** over a transmission medium (today an **optical or satellite link**)

Photons of light acquire a superposition state, that can represent an information of 1 or 0 simultaneously with a certain probability. **(QuBits).** Qubits super-fragile quantum state "collapses" to either *1* or *0* if tried to be observed by a hacker, leaving unmistakably trace of information tampering.

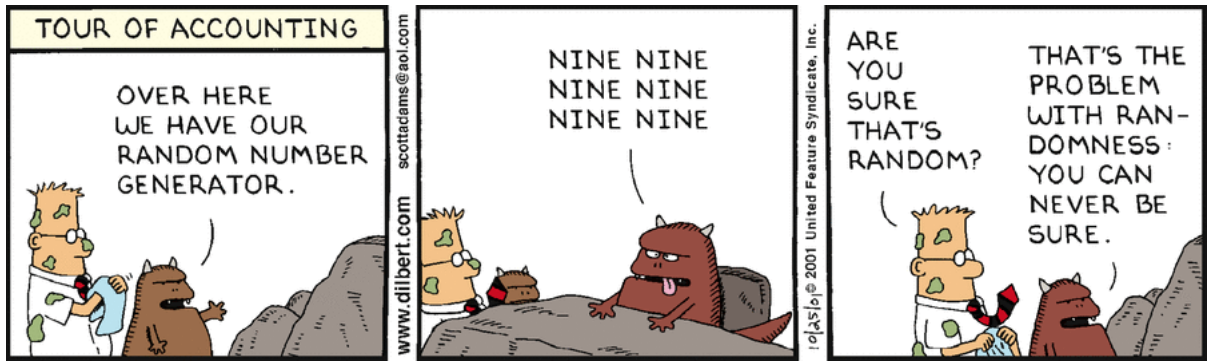


QRNG

Quantum Random Number Generators generate **true random numbers** with a high source of entropy using **unique properties of quantum physics**.

"*The inability to predict the numbers is not just based on complexity but it is in principle impossible to predict random numbers - one could say that even nature does not know these random numbers before they are produced*" (*)

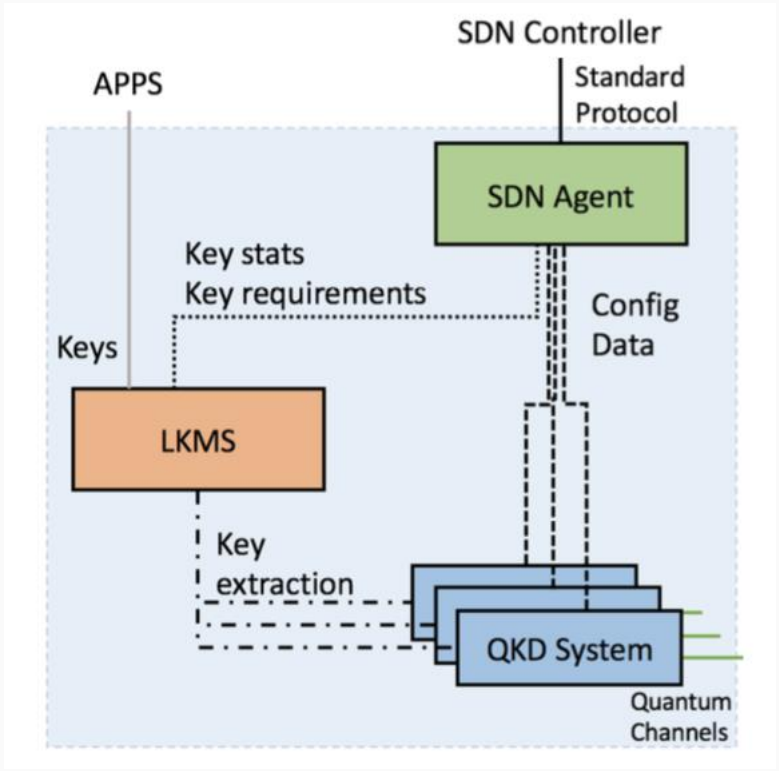
(*) European Quantum Flagship. Underlying Principles



Software Defined QKD Networks

OPEN QKD

Software Defined QKD Node



Control plane protocols and interfaces within a transport network

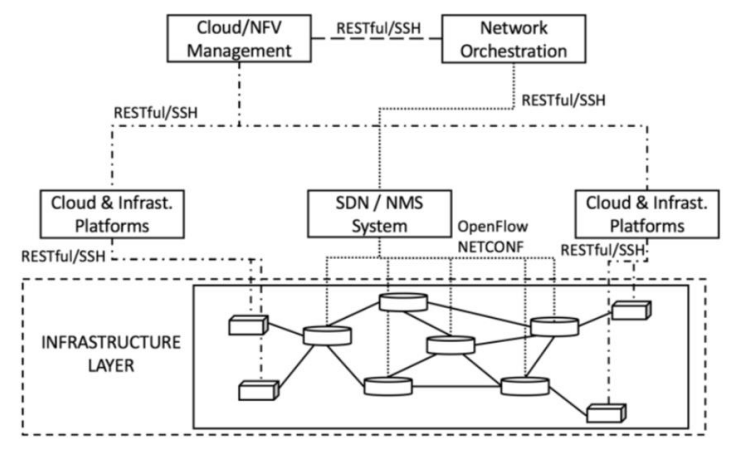
- **Software Defined Networks** (SDN) enables the **automation** of service provisioning within network operator infrastructures.
- With the **dynamic network requirements**, operators can not anymore deploy their services based on manual intervention or using proprietary vendor solutions.
- **Standard programmability** is key in the next-generation network infrastructure and any new technology must be integrated with this paradigm.

ETSI ITU IETF

Relevant use cases in 5G

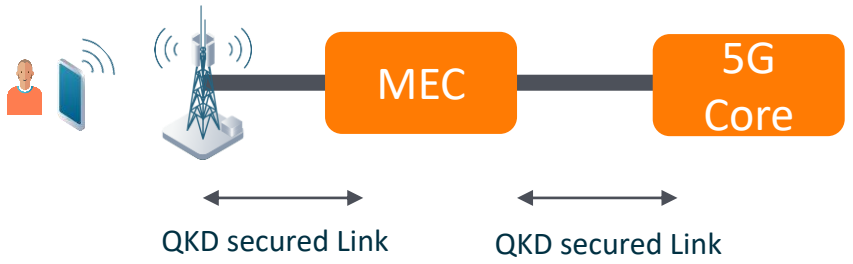
Management & Control plane protocols and interfaces within a transport network

- **Management and control plane** become critical in virtualization environments. QKD/QNRG keys will allow to securely handle any centralized operation, including the communications channels between **NFV platforms**, the communication between an **SDN controller** and a network device, etc.



Quantum Cryptography for 5G networks

- QKD play an important role securing transport services.
- This will allow encrypting connectivity from **base stations** to **MEC,** and/or **core** (e.g. for 5G), to incorporate quantum-safe security for end users' communications.



PUBLIC USE

Network domain Security & Privacy:

SDN helping in security

Proof of Transit (PoT):

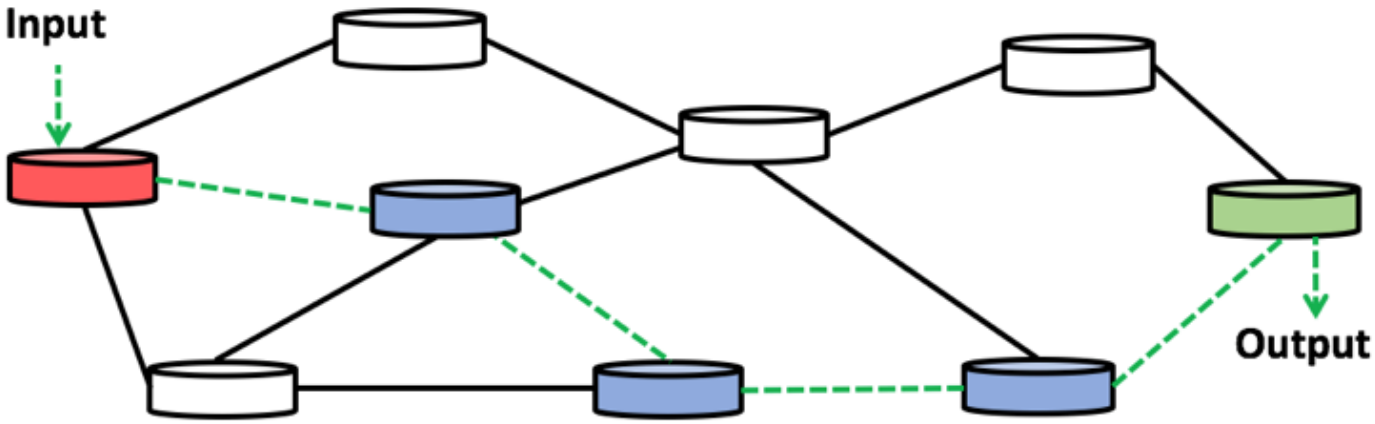
draft-brockners-proof-of-transit

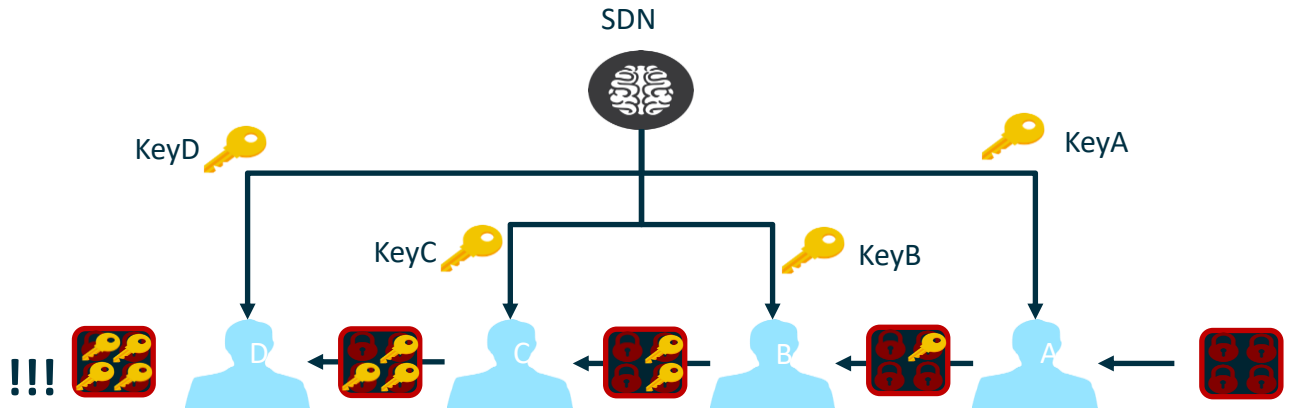
Methodology for verifying that specific traffic (e.g. a flow) traverses certain nodes across the network.

Their methodology is based on a double Shamir's Secret Sharing (SSS) technique, with a first polynomial kept secret and fixed, and a second polynomial changing it's constant value randomly from the source node

Can provide network liability for QoS, 5G slicing.

Can force traffic through security devices (encryptors, firewalls, Lawful interception, etc..)





IPSec IKE-less

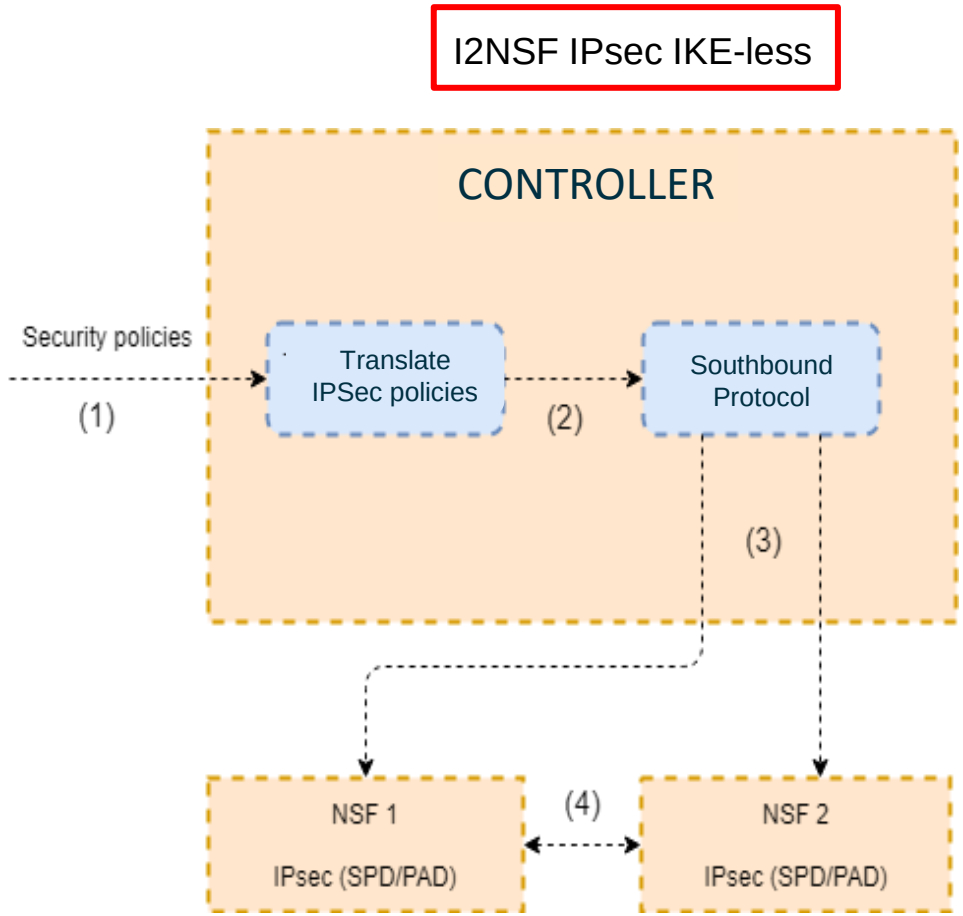
IPSec based on SDN I2NSF

IPsec architecture defines clear separation between the processing to **provide security services to IP** packets and the key management procedures to establish the IPsec Security Associations.

IPSec is a **key technology in 5G security:**

- Backhaul connectivity for several protocols (F1, eCPRI, GTP)
- Roaming based on IPX-Diameter

I2NSF defines a standard interface to distribute and configure on-demand keys to provide flexible, automated, fast deployment security network service.



https://datatracker.ietf.org/doc/draft-ietf-i2nsf-sdn-ipsec-flow-protection/

PUBLIC USE

Security Management and control:

AI/ML

Why do we need AI/ML in 5G?

- Data collection and analysis for ML is considered part of 5G technologies
  - R15 3GPP Network Data Analytics Function (**NWDAF**)
  - "Security Monitoring Analytics System" in **ENISA 5G threat Landscape** report
    - .."applies advanced ML techniques on the telemetry to perform advanced detection of security anomalies and emerging threats in the system"
- ML impacts in cybersecurity in 2 dimensions:
  - ML based tools :
    - Anomaly detection, Classification of attacks
    - spam, malware, phishing
  - ML based attacks*:
    - Leverage AI to improve malicious activities
      - malware: obfuscate from antivirus, avoid spam filters, use cloud AI services,
      - Penetration test: password guessing, vulnerability scans
    - Use AI to deceive AI
      - Manipulate data sources:
      - Adversarial networks (ML against ML- > Resilient ML)

*https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence

5G Cyber-range

- Security experts needs to ***learn*** how ML impact in their job
  - Use ML based tools to detect and mitigate attacks:
    - Understand the insights of a ML tool
      - Confidence levels, false positive, true negatives
  - Learn to live with AI based attacks:
    - Not an infallible but supplementary tool
    - Parametrization, compare different tools (ML or classical tools)
- Solution: Integrate ML tools in SPIDER* **Cyber-range** through:
  - ML Infrastructure to train & test customized ML models before exercises
  - Deliver ML-based attack detectors integrated in toolboxes to be utilised in Cyber-exercises

Telefónica

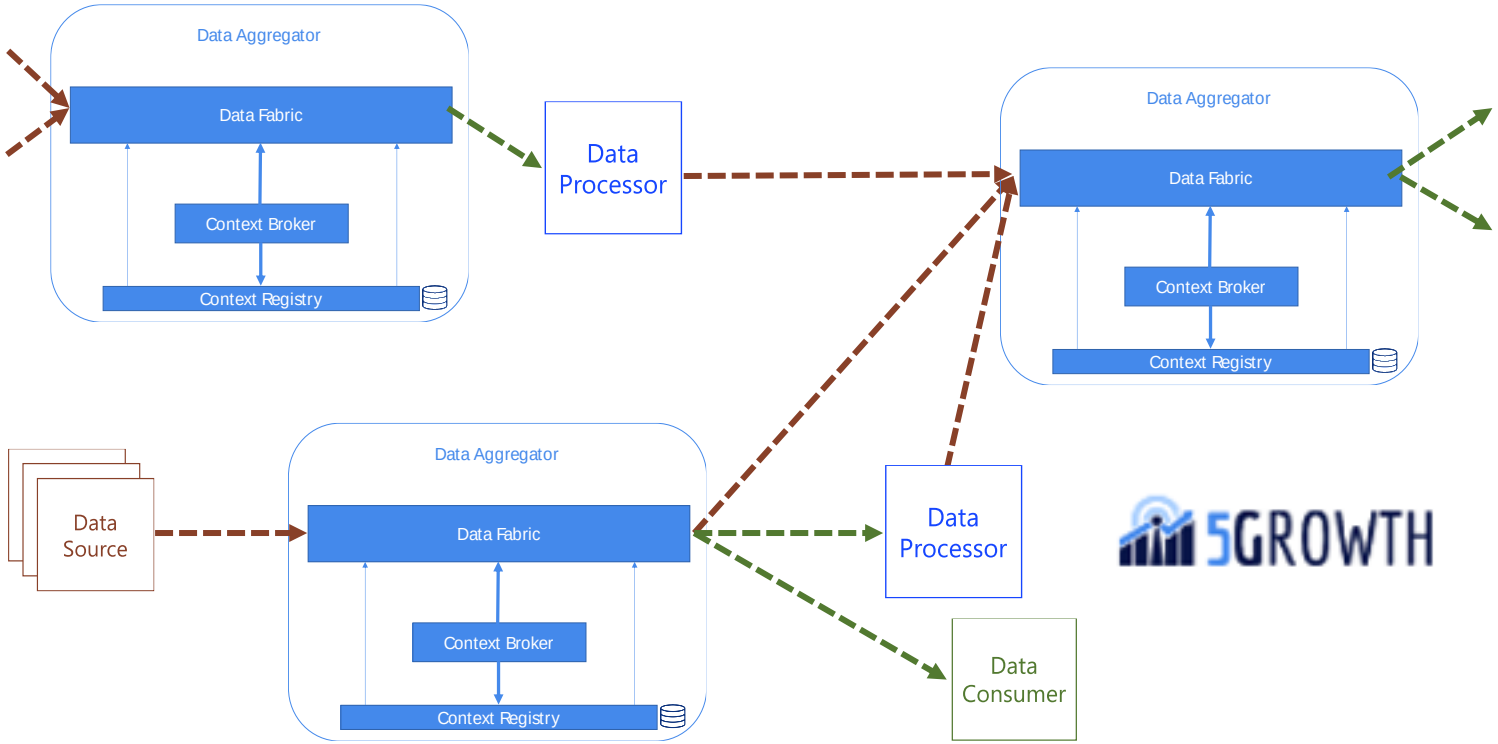
*https://spider-h2020.eu/

This project receives funding from the European Commission H2020 programme under Grant Agreement Nº 833685. The European Commission has no responsibility for the content of this presentation.

Data from the network is key for AI/ML

Moving to data flexible solution for data collection and aggregation

- Rely on aggregation nodes
  - Sources feed data
  - Consumers receive them
  - Aggregators map and integrate
- Based on metadata
  - Dynamic composition
  - Transport protocol agnostic
  - Telemetry data models
  - Knowledge ontologies
- Compositional patterns
  - Any element can play any role
  - AI / ML supported anywhere



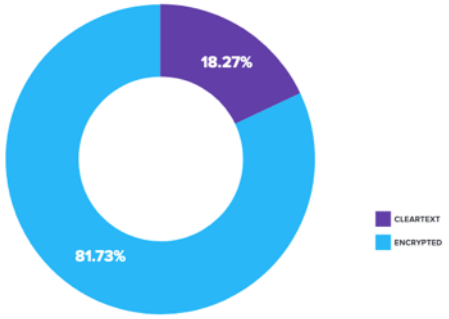
Example: Network protocols are evolving

..and the future is encrypted

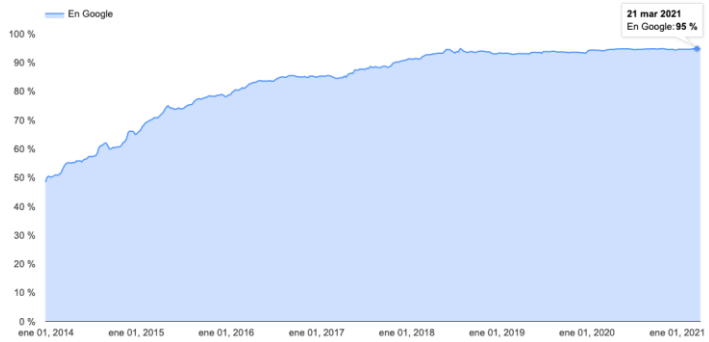
Layer 2 to 7

Lack of visibility **in all layers**

GPON, 3/4/5G Radio,..
MacSec,…
IPSec,…
DTLS, TLSv1.3, ESNI,…
QUIC, SSH, PGP, JWT, DoH / DoT



Telemetry.moziilla.org via f5.com



Google transparency report HTTPS

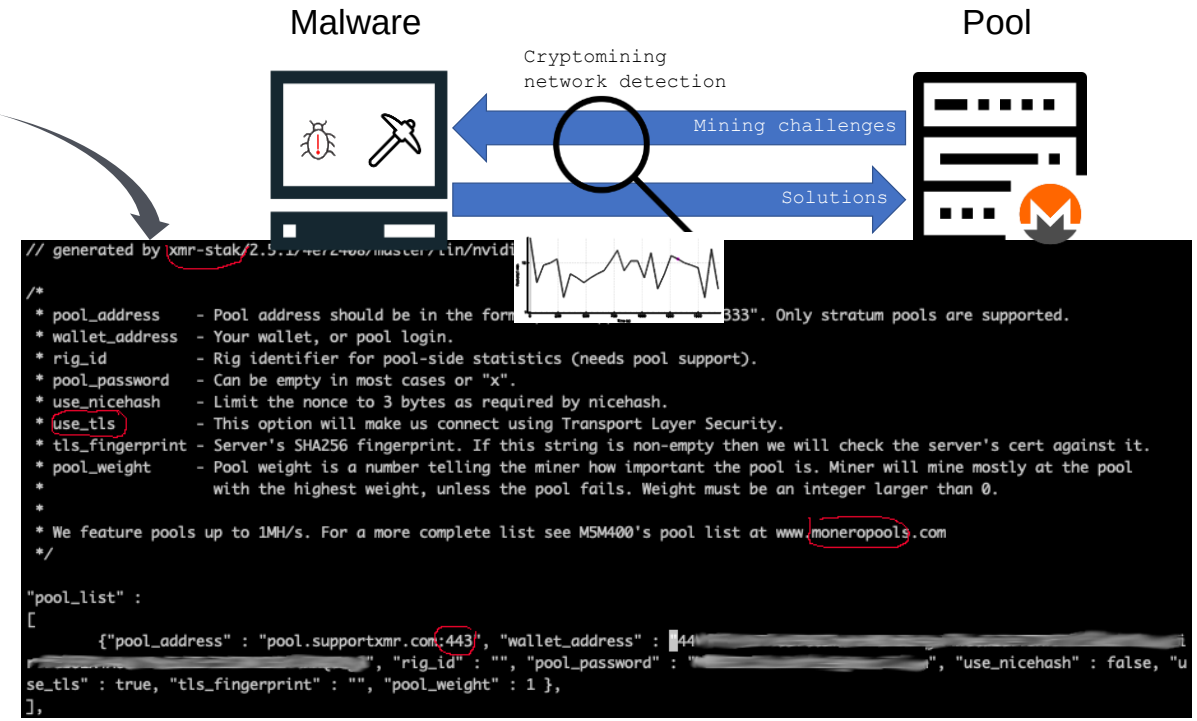
The evildoers know it

TLS easiest than ever (e.g. Let's encrypt)

Malware spreading (droppers, exploits, C&C, cryptomining)

Application layer attacks over HTTPS (XSS,CSRF,..)

DoT (DNS over TLS)
- Domain blocking, e.g. IWF
- DGA
- DoS



5G in not an exception and need new approach

Stand Alone will change 5G Core. *Security highly impacted*

Point of encryption

TLS → New SBA architecture

5G-AKA ← PDCP

Backhaul ← IPSec/MacSec

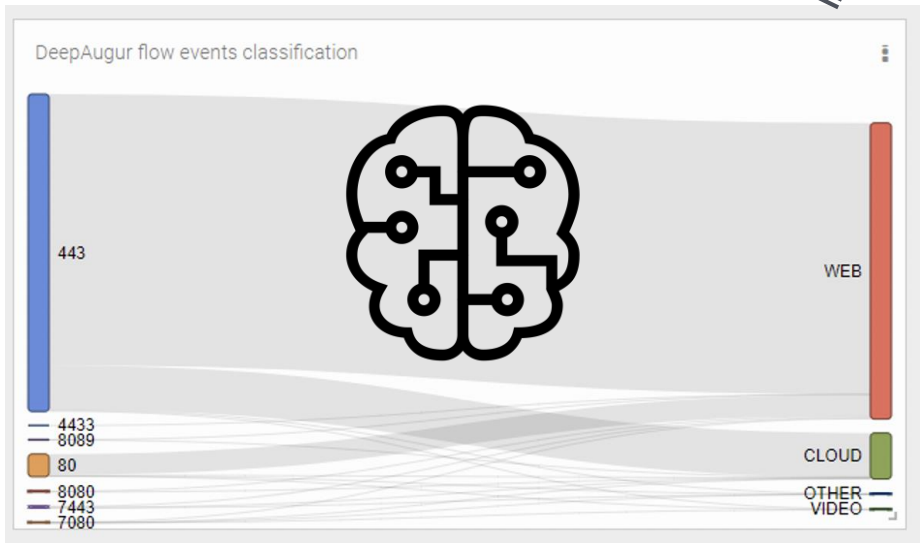
IPX ← JWE

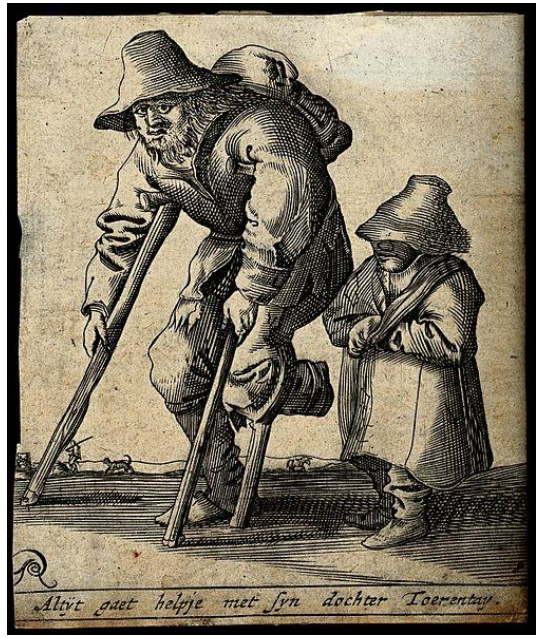
Current security technologies

Tailored to legacy protocols & architecture

Assume traffic visibility

Artificial intelligence





Telefónica

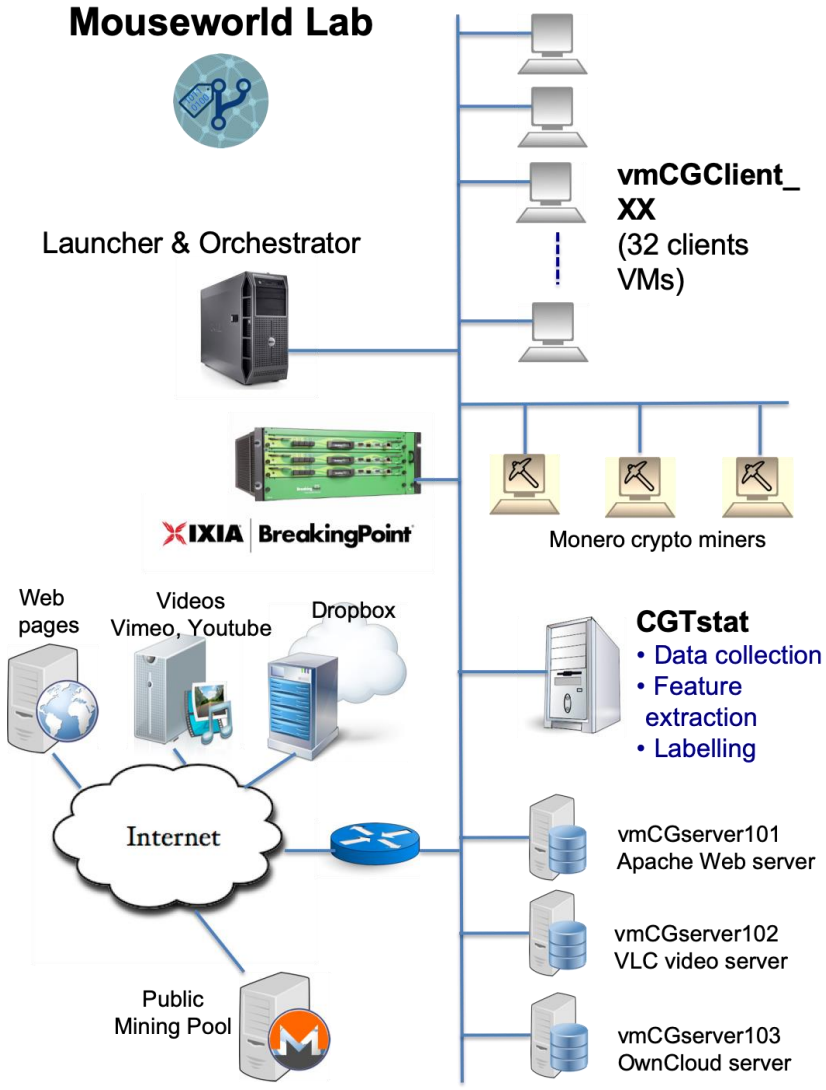
PUBLIC USE

How we evaluate all these technologies?

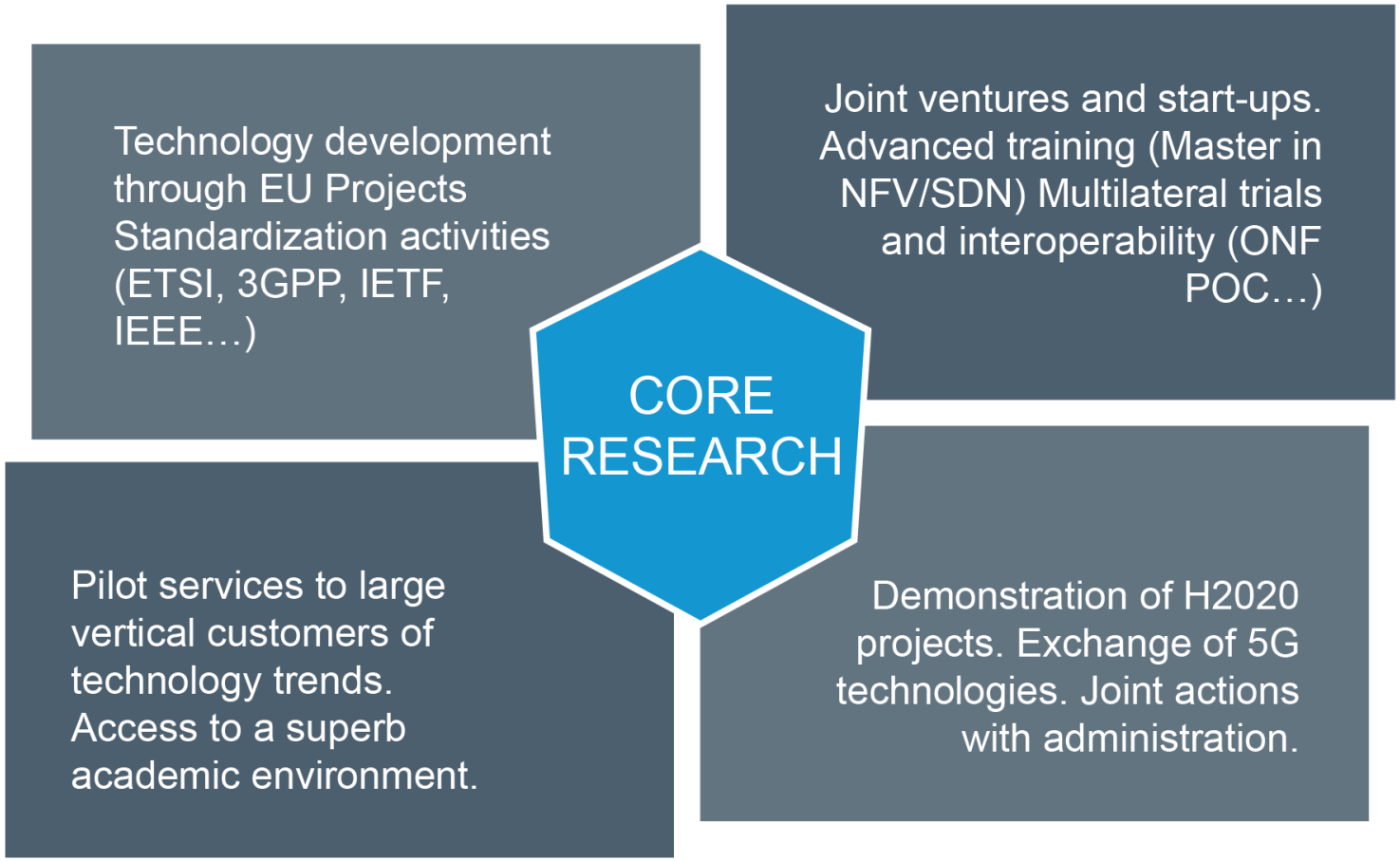
Mouseworld*

.. Synthetic Traffic and Beyond

- Traffic at all network segments
- Clients, servers, middleboxes and network functions of many natures
  - Plus raw traffic captures and other external sources
- Traffic analysis to produce (labelled) datasets
  - Flow aggregation and composition
- Train and validate
  - ML solutions, supervised and unsupervised
  - Data-driven modules (AI, Analytics…)
- Repeatable and controlled conditions and variants
  - SDN/NFV
  - Data infrastructure orchestration



*https://doi.org/10.1145/3230833.3233283



5TONIC

https://www.5tonic.org/

5TONIC is an **open co-creation laboratory** focusing in **5G technologies**, founded by Telefónica and IMDEA Networks and based in Madrid.

PUBLIC USE

Bringing it all together

A Vision for 5G and Beyond Security

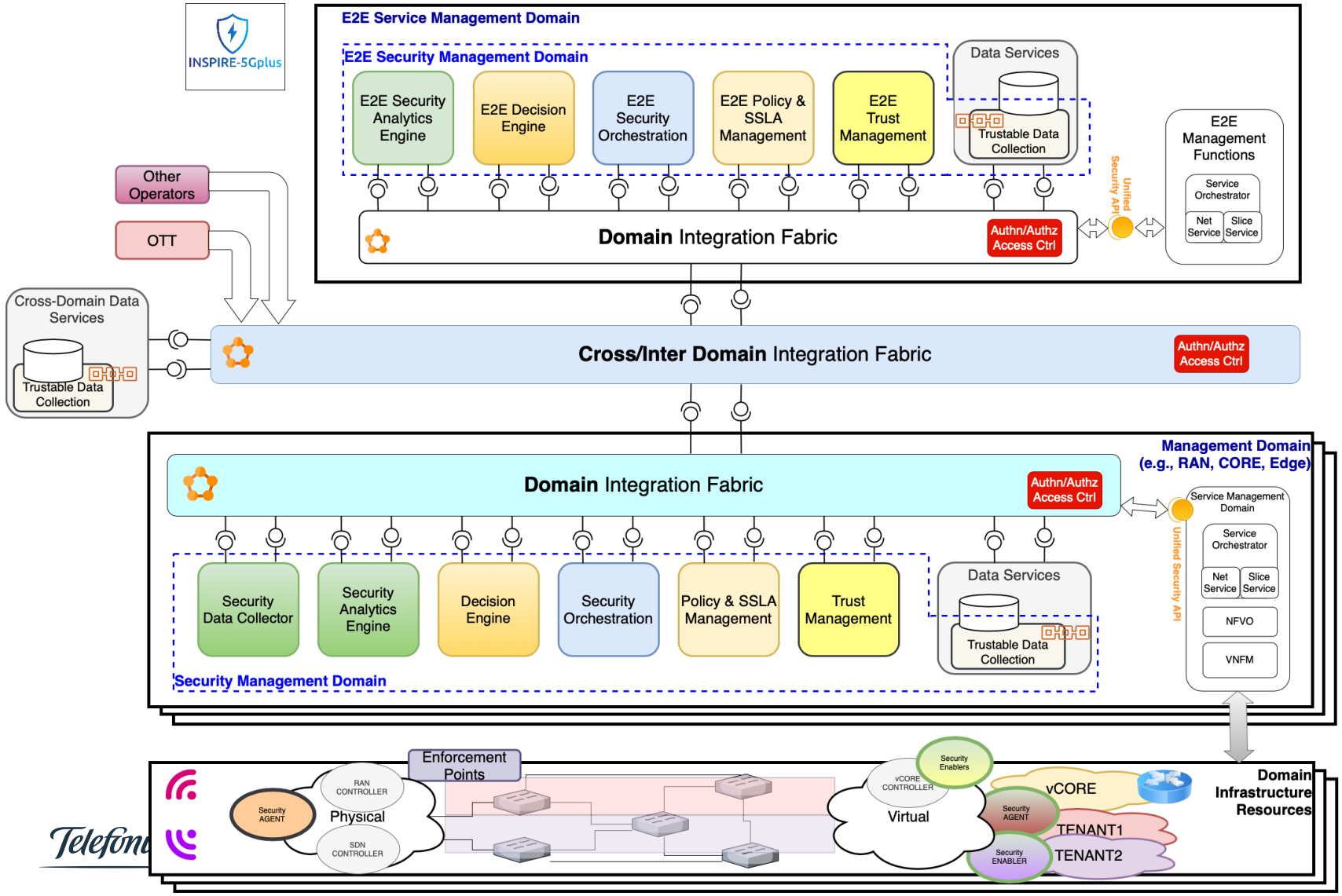
Intelligent Security and Pervasive Trust for 5G and Beyond (INSPIRE-5Gplus)

- Make a revolutionary shift
  - Devise and implement a **smart**, **trustworthy** and **liability-aware 5G security platform for future connected systems**, while contributing to its realization
- Foster adoption of most promising trends (e.g. SD-SEC, SECaaS, …) and technologies (e.g. AI/ML, TEE, ETSI ZSM)
  - **Develop new assets and models** to address some of the remaining challenges (e.g. adaptive slice security) or are completely new (e.g. proactive security)
- Move from Trust to Liability while ensuring conformance to what applies
  - Trust and liability will be fostered through integration of **novel mechanisms supporting confidence** between parties **and compliance** with regulation
- Deliver innovative and actionable results (methodologies, enablers, services)
  - For interested 5G-PPP ongoing projects (i.e., ICT-17, ICT-18 and ICT-19) to take advantage

Telefónica

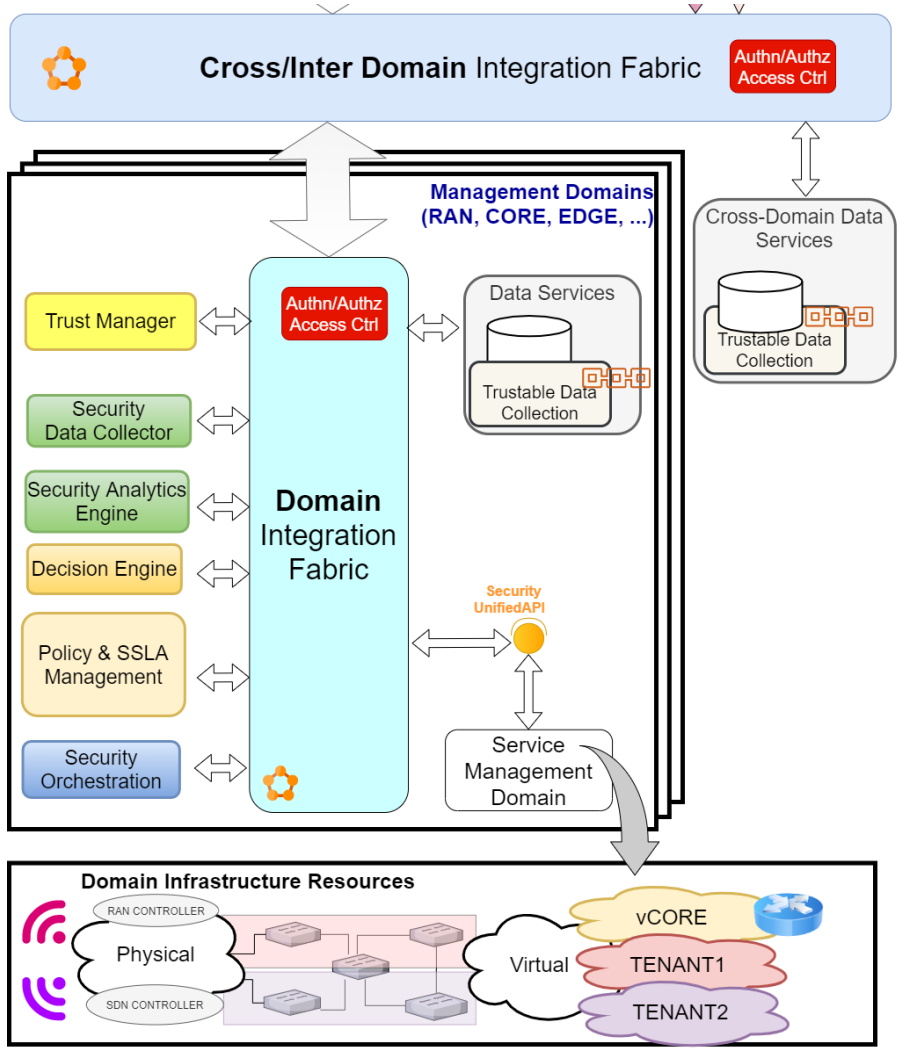
Acknowledgment:
The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement Nº 871808. The European Commission has no responsibility for the content of this presentation.

High-Level Conceptual Architecture



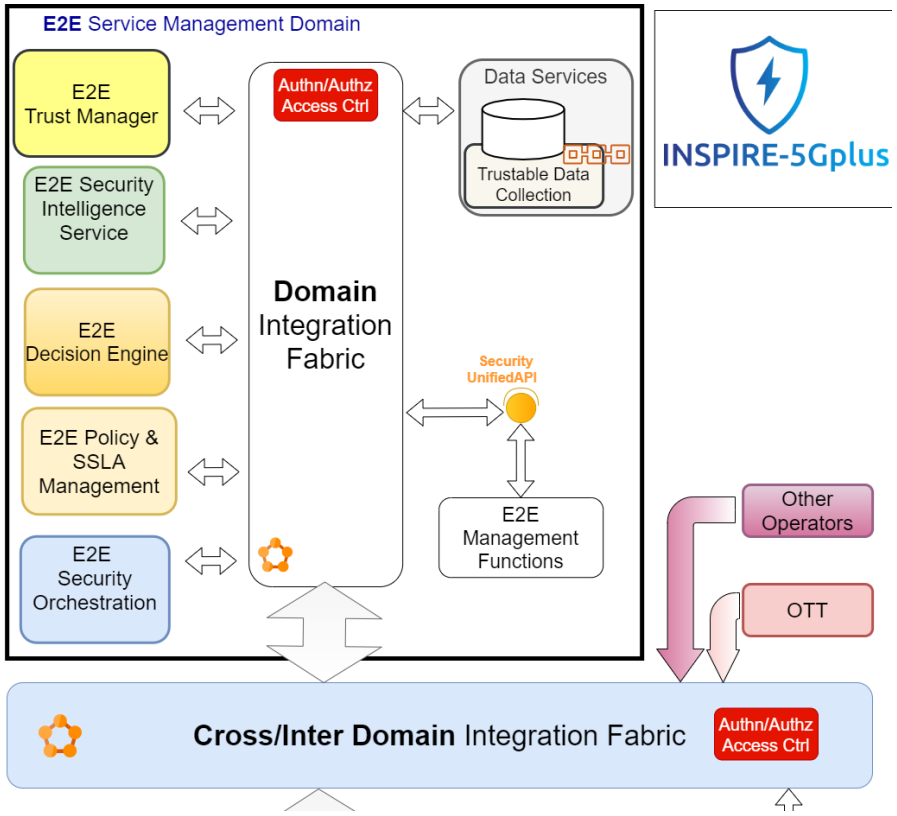
- **Compliant** with **ETSI ZSM** reference architecture
- **Separation** of sec. mgmt. concerns (SMDs + E2E SMD)
- **SBA** (Integration Fabric)

Security Management Domain (SMD)



- Security Data Collector (SDC)
  - Gather all the data coming from the security enablers at the domain level
- Security Analytics Engine (SAE)
  - Insights and predictions, with Anomaly Detection and Root Cause Analysis, on specific domain's security conditions (based on data from SDC).
- Decision Engine (DE)
  - Select the best decisions for securing a running targeted service. Mitigation actions based on Cognitive Long-Term
- Security Orchestrator (SO)
  - Interact with different SDN controllers, NFV MANO and security management services to enforce proactively or reactively the security policies, through the allocation, chaining and configuration of virtual network security functions (VSF)
- Policy and SSLA Management (PSM)
  - Provides a framework defining the language and semantics to define Security Service Level Agreement (SSLAs) based on security policies, and transforms into specific parameters
- Trust Manager (TM)
  - Various internal services for the trust related functions in the security framework.

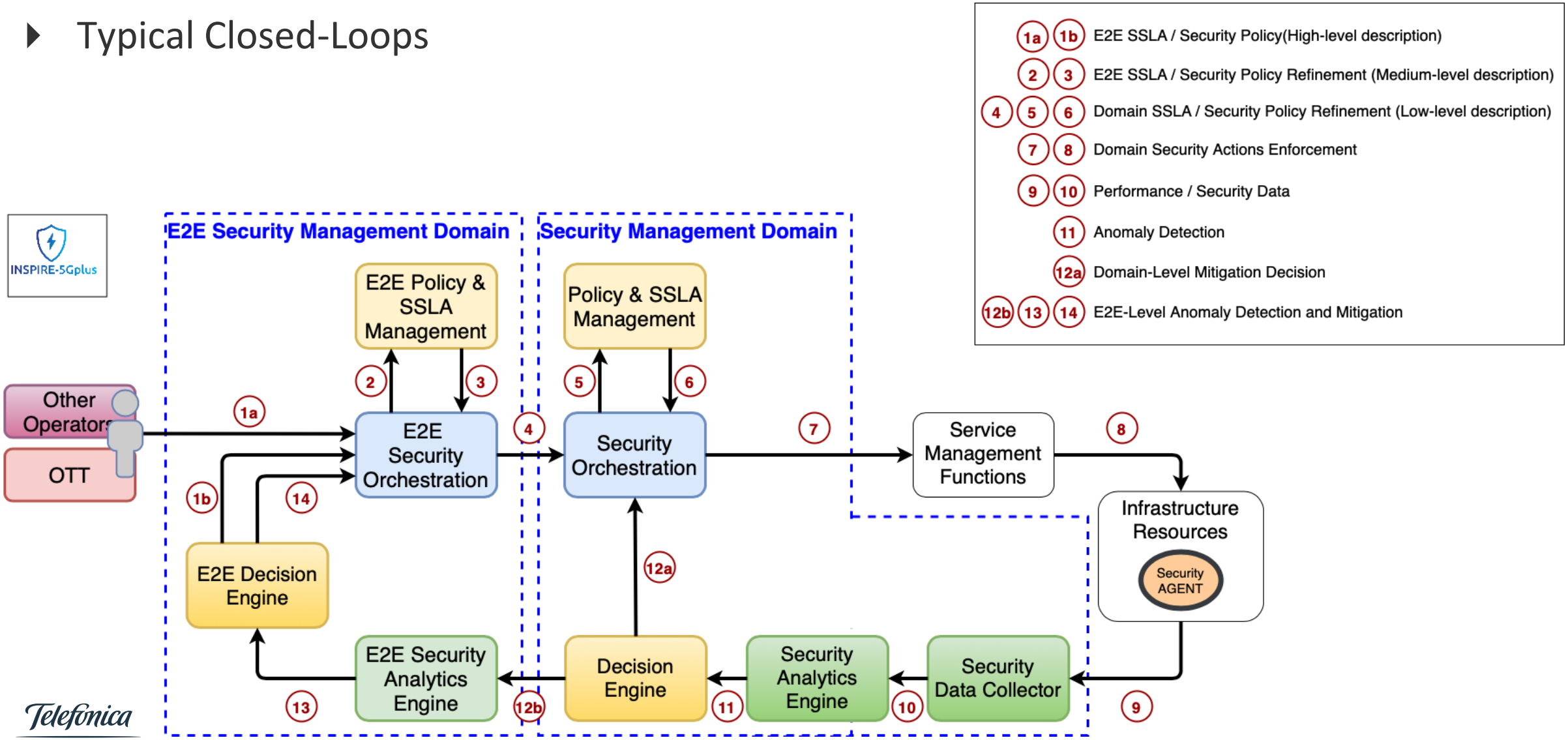
E2E SMD



- The **E2E SMD** is a special SMD that manages security of E2E services (e.g. E2E network slice) that span multiple domains
  - E2E Security Intelligence Engine (E2E SIE)
    - Cross-domain insights and predictions based on data collected, and stored in the Cross-Domain Data Service. from different domains.
  - E2E Decision Engine (E2E DE)
    - Manages the high-level security at the E2E level to adapt and propagate the security decisions across multiple domains.
  - E2E Security Orchestration (E2E SO)
    - Orchestrating and managing the different security enablers from multiple domains to cover the security requirements defined in E2E security policy. Interacts with the SOs at domain level.
  - E2E Policy and SSLA Management (E2E PSM)
    - Provides multi-level SSLA policy with conflict avoidance to prevent contradicting policies or requirements of previously deployed security services.
  - E2E Trust Management (E2E TM)
    - It can provide across-domain versions of trust functions by aggregating trust outputs of TMs in different domains and enriching them with inter-domain parameters.
- The integration fabric (at domain or interdomain level)
  - Facilitates the interoperation and communication between services provided by the different functional blocks, within a domain and across domains. It provides services to register, discover and invoke security management services

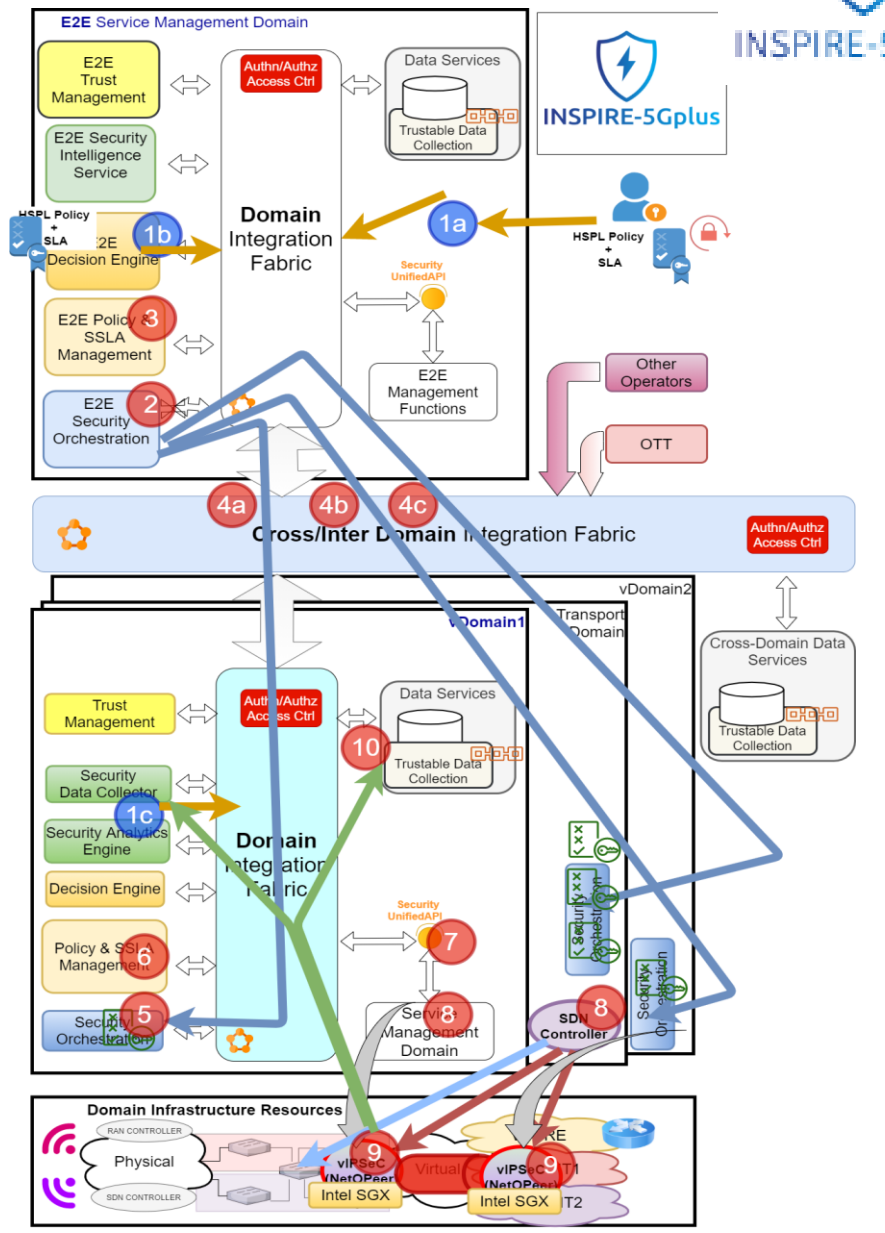
High-Level Conceptual Architecture

- Typical Closed-Loops



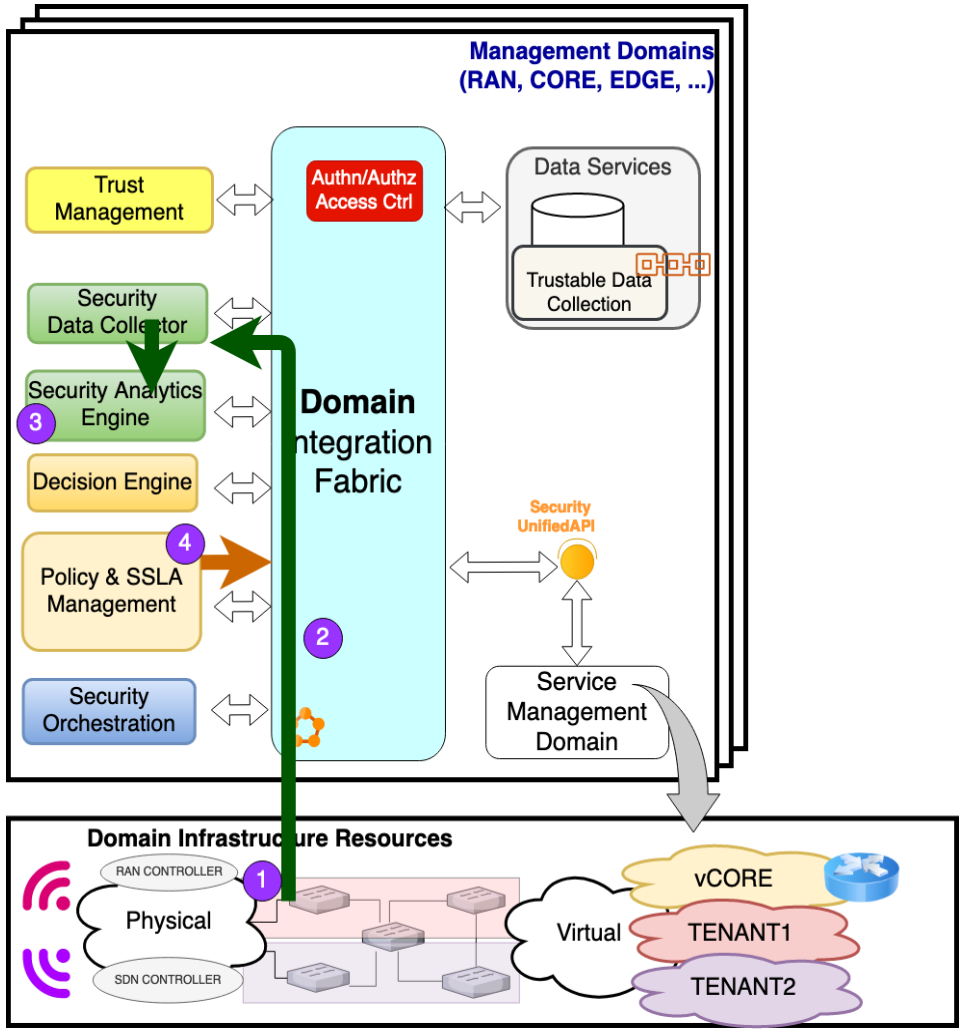
Illustrative UCs

- Orchestration of Cryptomaterial for Connections
  - Problem:
    - 5G verticals use slices across multiple domains to exchange sensitive data.
    - E2E slices cryptographic protection provide privacy, but static/long-lived keys and certificates generate risk.
  - Solution
    - Zero Touch VNF-based E2E encryption over 5G MECs with centralized SDN key distribution and secure enclaves on the MEC to protect cryptographic material usage.
    - Tools: PoT, I2NSF IPSec, TEE



Illustrative UCs

- Network Attacks over Encrypted Traffic in SBA
  - Problem:
    - 5G adopts pervasive E2E encryption
      - Service Based Architecture (SBA) signalling traffic with mTLS and exposed REST API
      - DNS over HTTPS (DoH)
      - Applications within the Data plane (QUIC or HTTP/3)
    - Reduce security monitoring capacity
  - Solution
    - Extend security monitoring tools to be capable of analysing encrypted traffic
    - Tools: Mouseworld to train ML model, data aggregation, TEE



Thank you

patricia.diezmunoz@telefonica.com
antonio.pastorperales@telefonica.com


Telefónica