ETSI Security Conference 2022

INSPIRE-5Gplus: Vision on Security Beyond 5G

Antonio Pastor (Telefonica)

Vincent Lefebvre (Tages Solidshield)

05/10/2022

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

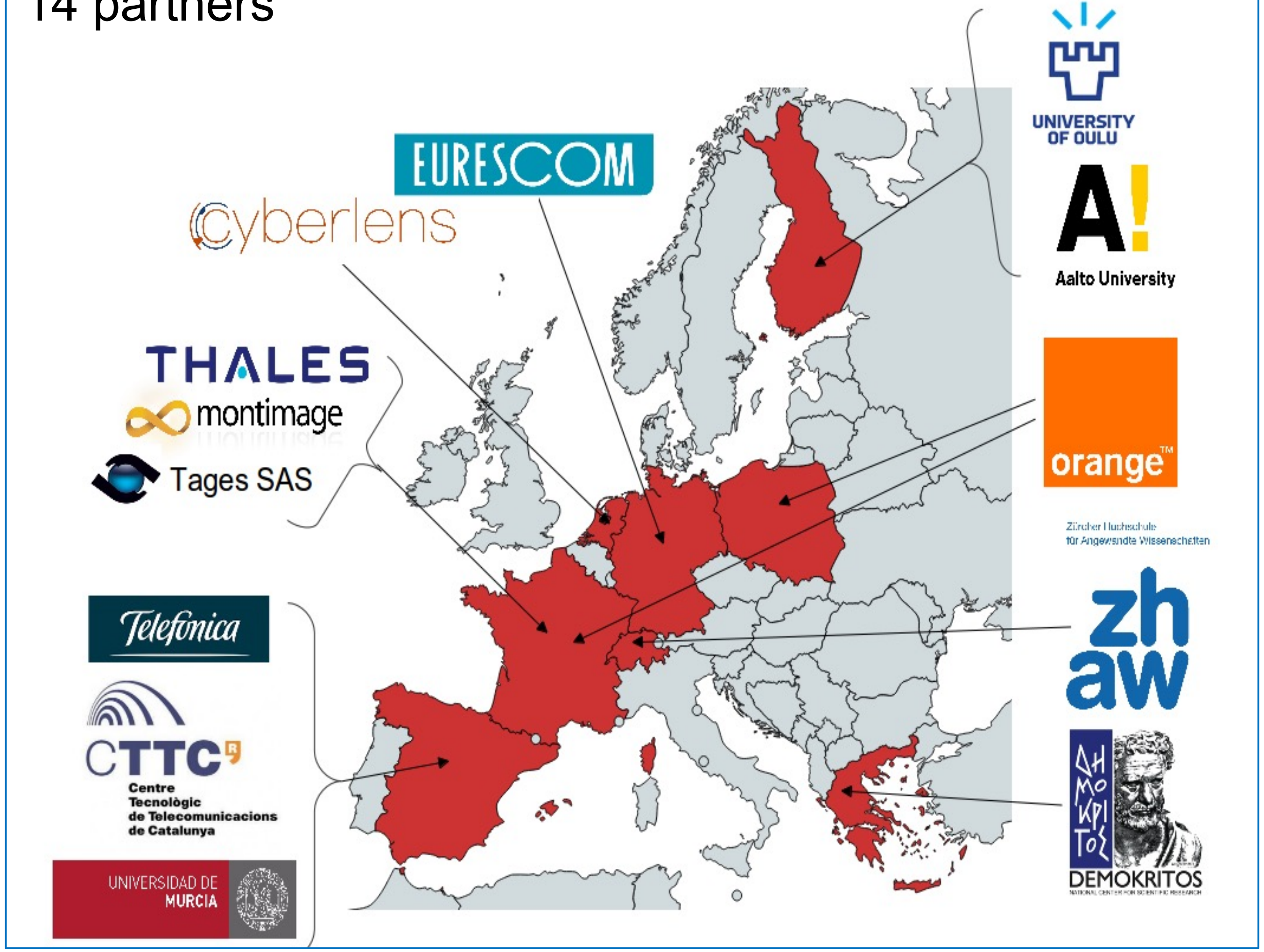
Project Coordinator

Eurescom, Germany

Technical Manager

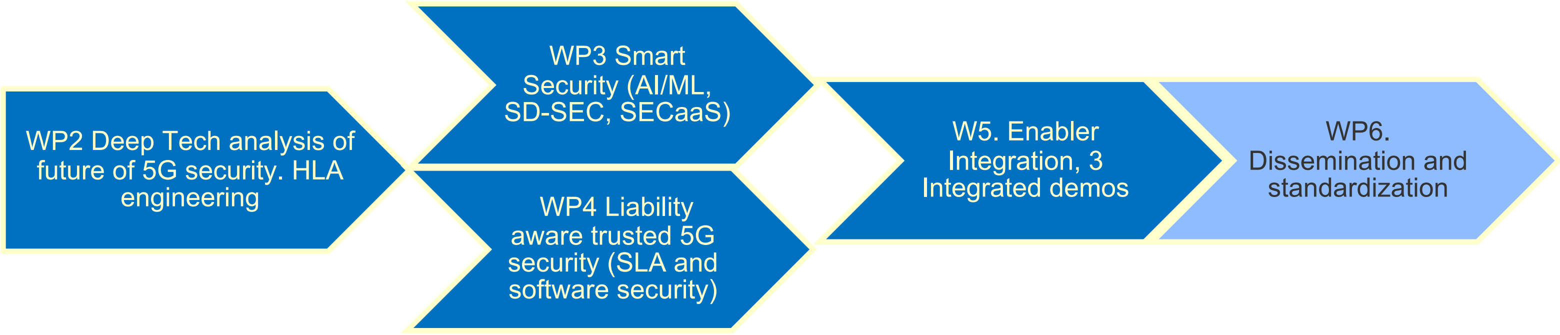
Thales, France

14 partners



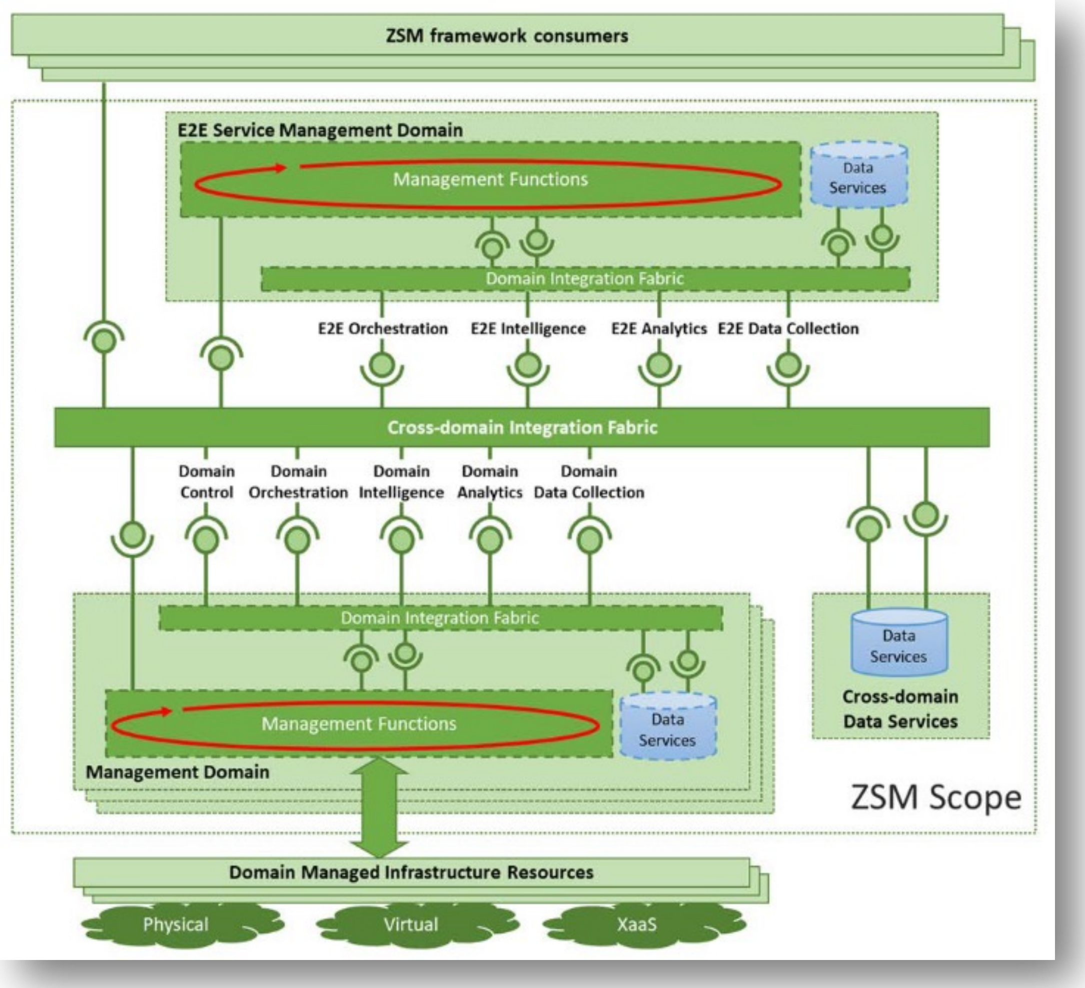
INSPIRE-5Gplus Vision and work plan

- INSPIRE-5Gplus = Intelligent Security and Pervasive Trust for 5G and Beyond
- **The vision**:
  - **End-to-End** Security, Trust and Liability management
  - Devise and implement a **AI/ML-backed, trustworthy and liability-aware 5G security HLA and platform.**
  - Leverages and fosters adoption of most promising of ETSI ZSM, AI-ML, TEE, DLT, SD-SEC and SECaaS
- **The plan**:
  - Identify **security and trust and liability gaps** remaining challenges (e.g. adaptive slice security) as well as new trends (e.g. proactive security)
  - **Design and/or progress existing partners 43 enablers** (e.g., E2E decision engine, MTD controller, Security orchestrator, Policy framework, vAAA, CAM lightweight auth, I2NSF IPSEC, data collector, Security Analytics Engine, data collector, Security analytics framework, Proof of Transit, TRAIL, Systemic software security and liability) interacting at all layers and delivering security, trust and liability functions.
  - Enablers integration efforts in UC definition and Demos, in representative and interconnected testbeds.
  - Deliver **actionable results** (**architecture, deep tech deliverables, enablers, use case demos**)


WP2 Deep Tech analysis of future of 5G security. HLA engineering
WP3 Smart Security (AI/ML, SD-SEC, SECaaS)
WP4 Liability aware trusted 5G security (SLA and software security)
W5. Enabler Integration, 3 Integrated demos
WP6. Dissemination and standardization

INSPIRE-5Gplus design principles

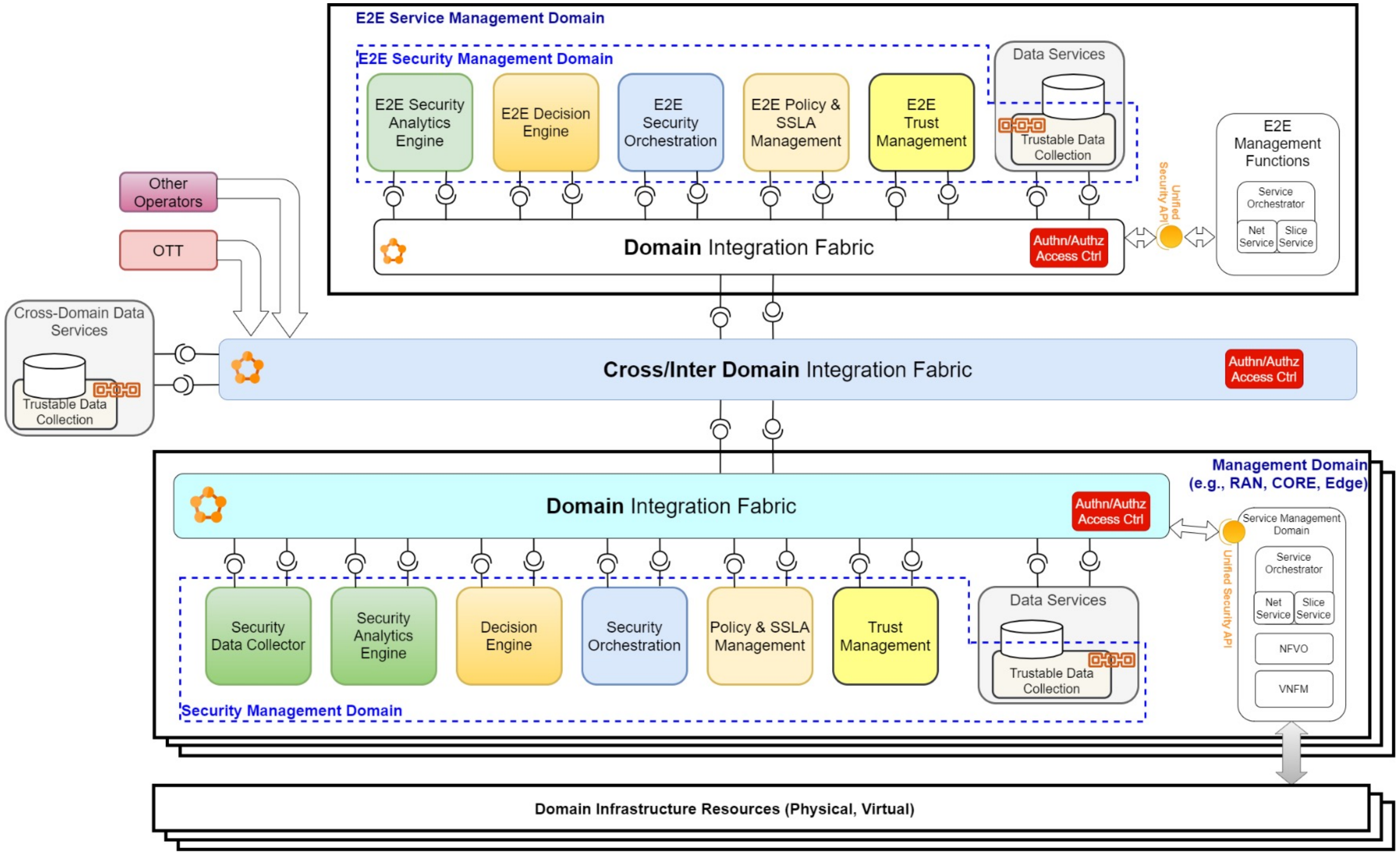
- Security Framework “inspired” by ETSI ZSM reference framework
  - Multi-domain support
  - E2E and domain management
  - Closed loop automation at multiple levels
  - Interconnection through integration fabrics
- Plus specific demands
  - Focus on 5G domains (e.g. RAN, Core, Transport, Edge)
  - Supported by security Infrastructure resources (probes and DPIs, etc..)
  - Trust & Liablity concepts



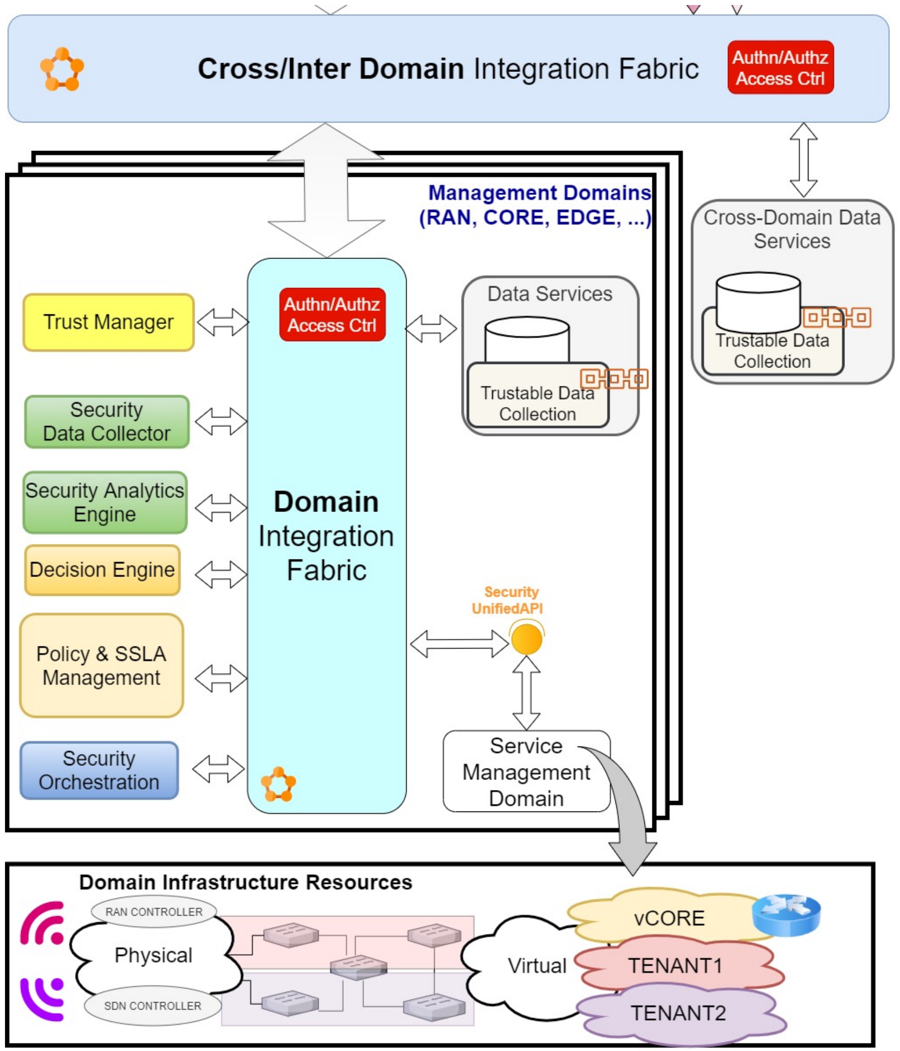
INSPIRE-5GPlus High-level architecture

Security Management Domains (SMDs)

- Supports the separation of security management concerns. (Granular, transparent and multi SMD traversal)
- Each SMD is responsible for intelligent security automation of resources and services within its scope.
- End-to-End (E2E) service SMD manages and orchestrates security of end-to-end services, e.g., network slices that span multiple domains.


E2E Service Management Domain
E2E Security Management Domain
E2E Security Analytics Engine
E2E Decision Engine
E2E Security Orchestration
E2E Policy & SSLA Management
E2E Trust Management
Data Services
Trustable Data Collection
E2E Management Functions
Service Orchestrator
Net Service
Slice Service
Unified Security API
Domain Integration Fabric
Authn/Authz Access Ctrl
Other Operators
OTT
Cross-Domain Data Services
Trustable Data Collection
Cross/Inter Domain Integration Fabric
Authn/Authz Access Ctrl
Management Domain (e.g., RAN, CORE, Edge)
Domain Integration Fabric
Authn/Authz Access Ctrl
Service Management Domain
Service Orchestrator
Net Service
Slice Service
NFVO
VNFM
Unified Security API
Security Data Collector
Security Analytics Engine
Decision Engine
Security Orchestration
Policy & SSLA Management
Trust Management
Data Services
Trustable Data Collection
Security Management Domain
Domain Infrastructure Resources (Physical, Virtual)

Security Management Domain (SMD)



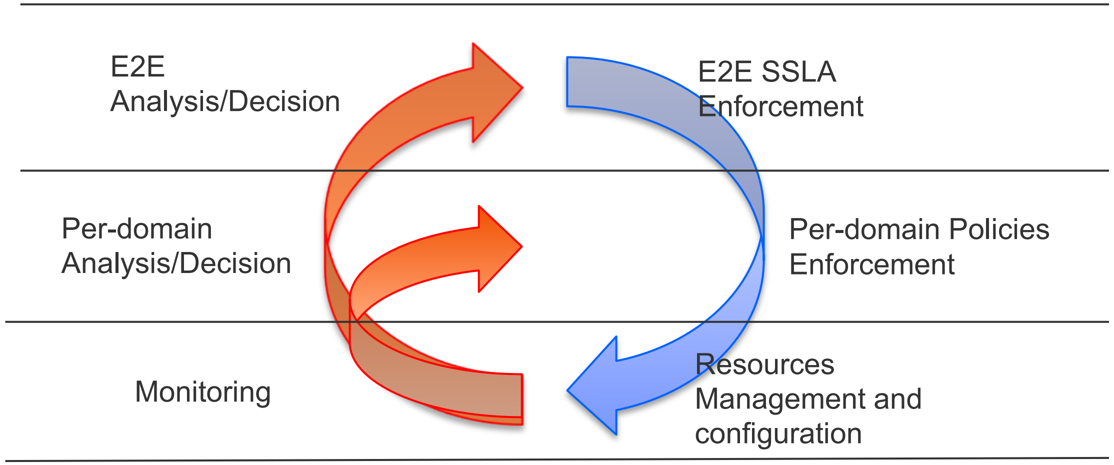
Cross/Inter Domain Integration Fabric
Authn/Authz Access Ctrl
Management Domains (RAN, CORE, EDGE, ...)
Cross-Domain Data Services
Trustable Data Collection
Trust Manager
Authn/Authz Access Ctrl
Data Services
Trustable Data Collection
Security Data Collector
Security Analytics Engine
Domain Integration Fabric
Decision Engine
Security UnifiedAPI
Policy & SSLA Management
Security Orchestration
Service Management Domain
Domain Infrastructure Resources
RAN CONTROLLER
Physical
SDN CONTROLLER
Virtual
vCORE
TENANT1
TENANT2

- 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.

INSPIRE-5GPlus Closed loop

- Each SMD, including the E2E service SMD, comprises a set of functional modules that operate in an **intelligent closed-loop** way.

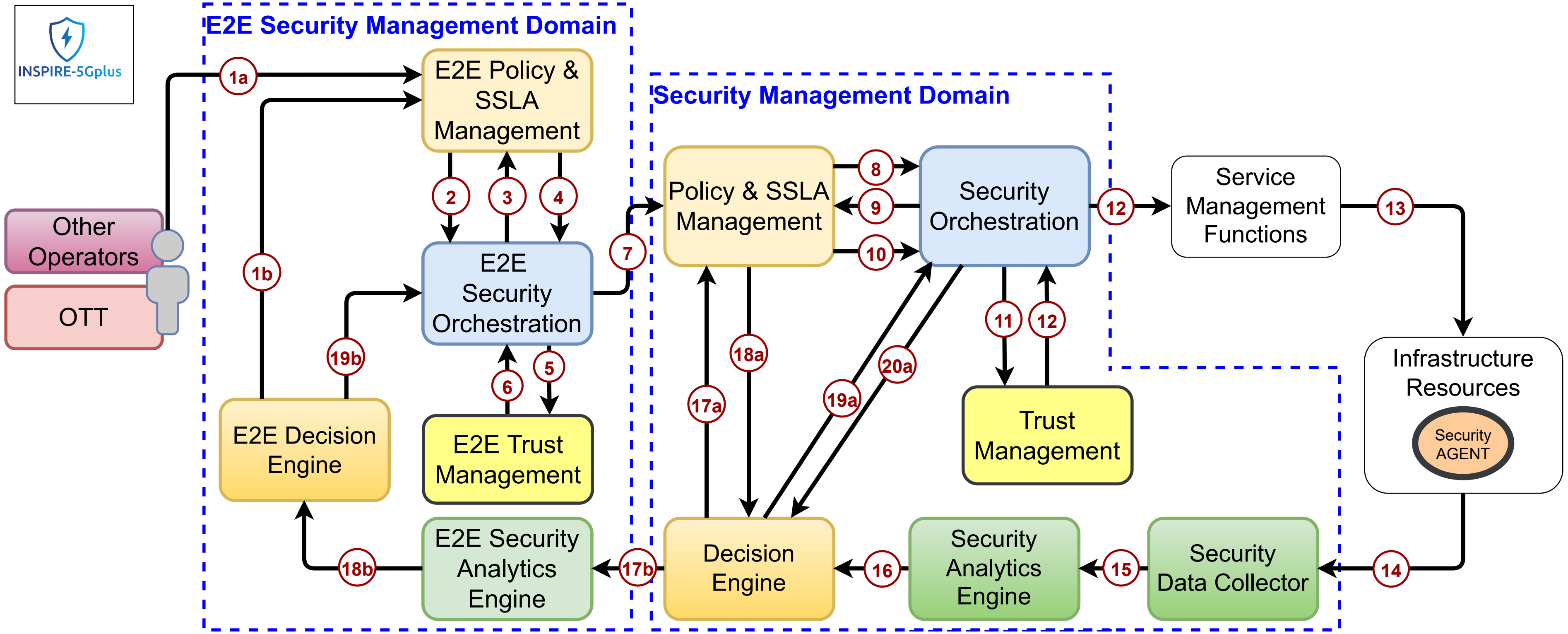
- It provides a software-defined security orchestration and management that enforces and controls security policies of network resources and services in real-time.



INSPIRE-5GPlus typical Closed loop

INSPIRE-5Gplus

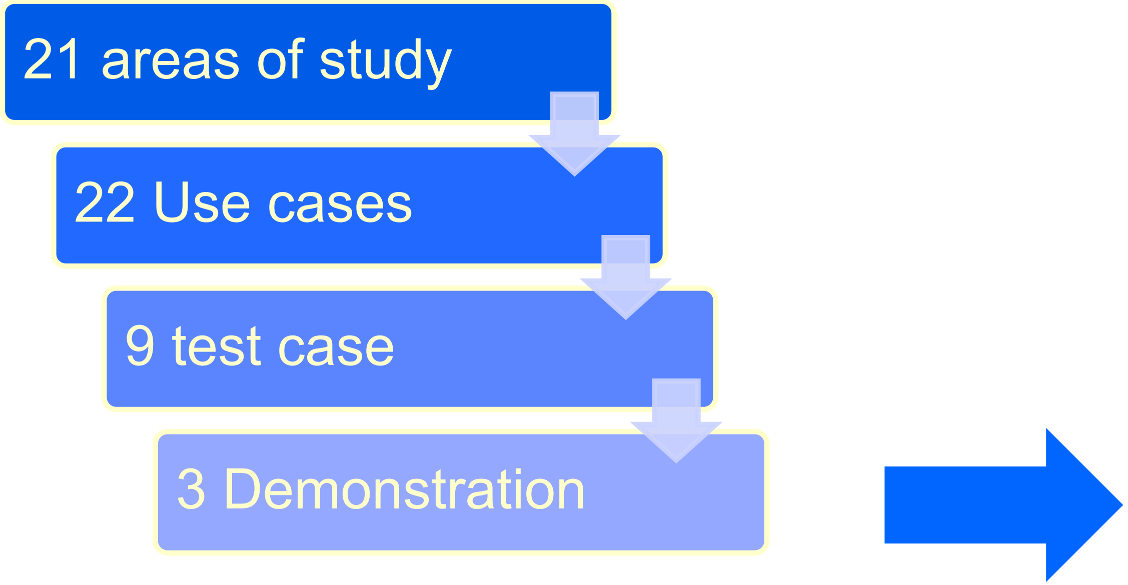
1a 1b	E2E SSLA / Security Policy(High-level description)
2 3 4	E2E SSLA / Security Policy Conflict Checking & Refinement (Medium-level description)
5 6	E2E Trust Scores retrieval
7 8 9 10	Domain SSLA / Security Policy Conflict Checking & Refinement (Low-level description)
11 12 13	Domain Trust Scores Retrieval & Security Actions Enforcement
14 15	Performance / Security Data
16	Anomaly Detection
11	Anomaly Detection
17a 18a 19a 20a	Domain-Level Mitigation Decision
17b 18b 19b	E2E-Level Anomaly Detection and Mitigation



From Security Gaps to Demos

- The initial Security Gap Analysis stated 21 areas of progress.
- This analysis guided to <u>22 use cases</u>, around specific technology domains
- Converged in 9 test Cases.
- A final reduced set of **3 “master” Demos,** illustrating the main outcomes of the project

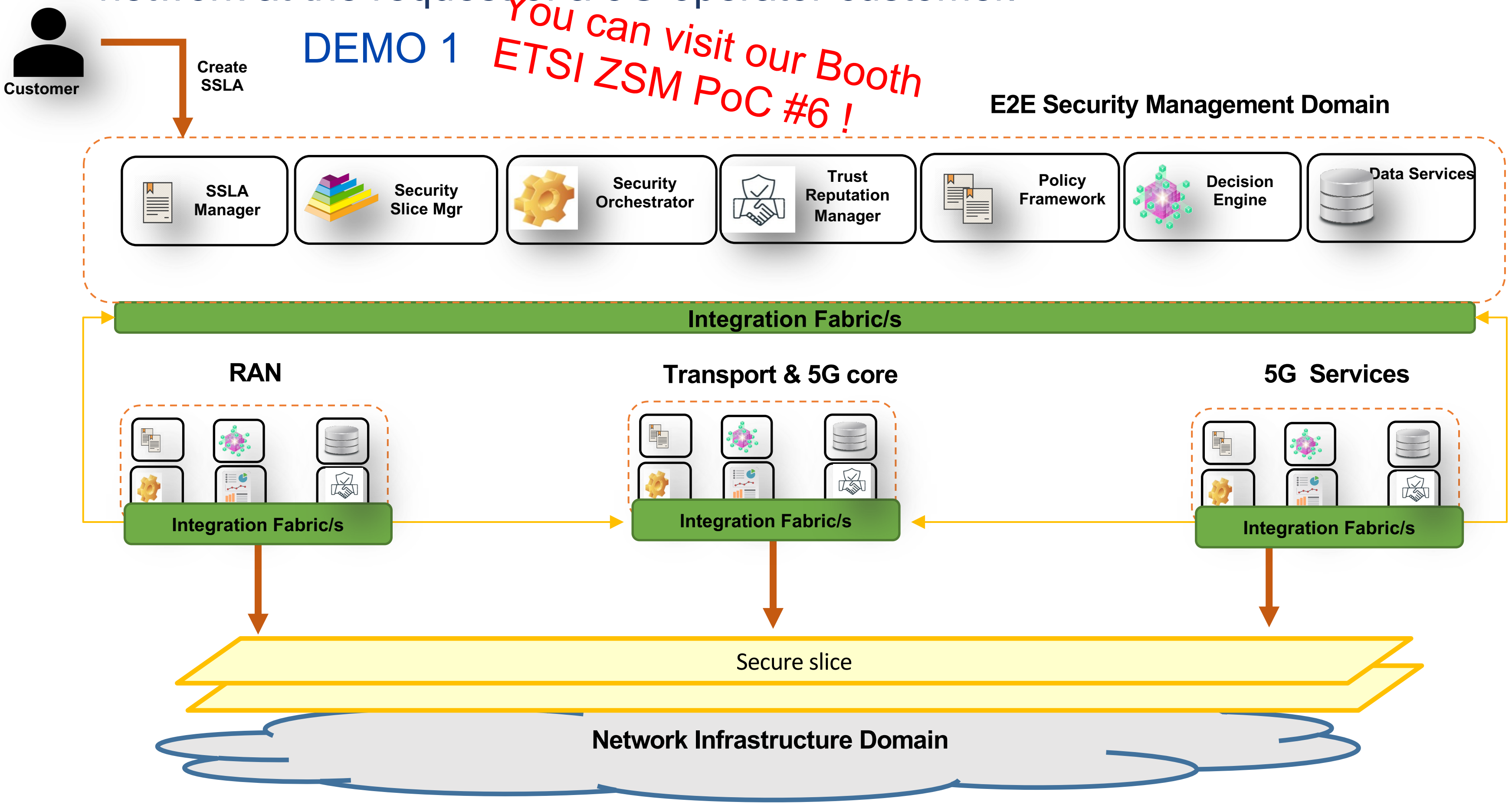
Authentication
DynamicLiability
CyberMimicDefence
SecuringArtificialIntelligence
VNF
Security
Liability
NFVI
SDSEC
MTD
Isolation
MANO
DLT
CCAM
TrustModels
SECaaS
SDNsecurity
Automation
MECsecurity
TrustedExecutionEnvironment
Verticals
MachineLearning
SecuritySLA
SecureRadioAccess
RootCauseAnalysis
DataSharing
CyberThreatIntelligence
ZeroTouchServiceManagement
ArtificialIntelligence



- DEMO 1 dynamic composition of Security Functions and their management with Security SLAs
- DEMO 2 On-Demand Security with the delivery of associated proven evidences of the security enforcement at a SSLA
- DEMO 3 Moving Target Defense against a DoS attack

INSPIRE-5Gplus Demos

1. A network slice with **specific Security Service Level Agreements (SSLAs) is instantiated** in a 5G network at the request of a 5G operator customer.



2. The **SSLA includes** 5G service **protection** scenario for the communication **between the User Equipment (UE) and a 5G service cloud** domain distributed over separate SMDs (e.g. RAN, Core, Cloud services).

3. The SSLA enforcement **will involve interaction with the different domains to deploy** the network slice and some **security solutions** (i.e., channel protection with IPSec or TLS and different assets monitoring).

4. A **closed loop reaction will automatically mitigate attacks** to ensure the SSLA compliance.

Complex demo with more than **20 enablers integrated**:

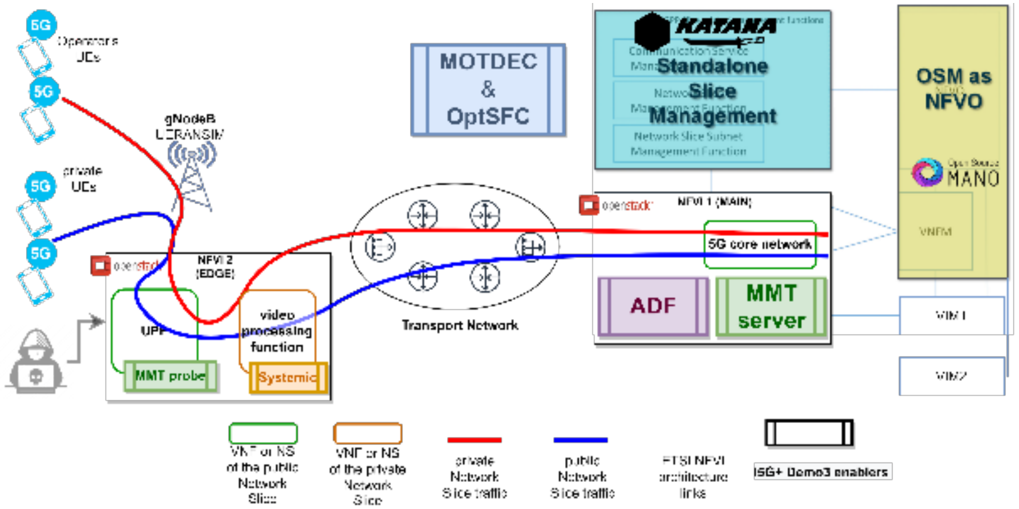
SSLA Manager, Security Orchestrator, Integration Fabric, Policy Manager, Decision Engine, V2X DoS detector, cryptomining detector, I2NSF IPsec, DTLS, etc…

Demand the use of **ETSI ZSM framework**

INSPIRE-5Gplus Demos

- DEMO 2 demonstrates the outcome of the researches made on Trust, Liability and Accountability and notably the concept of **On-Demand Security with the delivery of associated proven evidences** of the security enforcement at a SSLA (e.g., isolation) and the good operating conditions of Security Enablements.
  - The Demo 2 covers relevant enablers related with **Liability and accountability**
  - **Software hardening key enabler** for liability aspects (more in next slide)

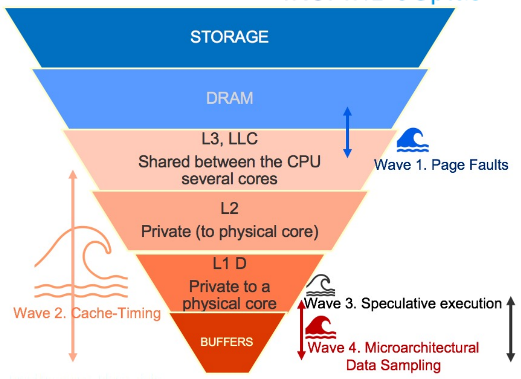
- DEMO 3 demonstrates the interactions of several enablers, endowing a **Moving Target Defense against a DoS attack**. It brings together AI/ML driven decision making, network monitoring, security incident detection and security orchestration to lay out a n integrated scenario for end-to-end slice protection.
  - improves the network's resilience against attacks, by effectively protecting network slices through dynamic reconfiguration of 5G infrastructure properties
    - TCP connections life migrations or the re-instantiation and the migration of VNFs and NSs
  - Integration a MTD and Slice managers and Software harding


5G
Operators UEs
5G
gNodeB UERANSIM
5G
private UEs
5G
openstack
NFVI 2 (EDGE)
UPF
MMT probe
video processing function
Systemic
MOTDEC & OptSFC
Transport Network
KATANA
Communication Service Management Function
Network Slice Management Function
Network Slice Subnet Management Function
Standalone Slice Management
openstack
NFVI 1 (MAIN)
5G core network
ADF
MMT server
OSM as NFVO
Open Source MANO
VNFM
VIM1
VIM2
VNF or NS of the public Network Slice
VNF or NS of the private Network Slice
private Network Slice traffic
public Network Slice traffic
ETSI NFVI architecture links
ISG+ Demo3 enablers

Works on Software Security

INSPIRE-5Gplus

- **SWOT-inspired analysis of TEEs for Telecom Industry use**
  - Initial deliverable D2.1: Practical use considerations, different models and “TCB gap”.
  - Mid-term deliverable D2.2: Survey of SGX-targeted SCAs and their criticality in the telecoms industry
    - With ETSI Secure VNF Bootstrappping protocol (e.g., From GS NFV-SEC-V3.1.1), no single SCA can succeed.
  - Final period upcoming SWOT publication:
    - Filled TCB gap, weakened weaknesses, novel risks (costs, evil TCB, blind DoS by DRAM bit flipping), massive resear


STORAGE
DRAM
L3, LLC
Shared between the CPU several cores
L2
Private (to physical core)
L1 D
Private to a physical core
BUFFERS
Wave 1. Page Faults
Wave 2. Cache-Timing
Wave 3. Speculative execution
Wave 4. Microarchitectural Data Sampling

- **Progress of SOLIDSHIELD’s SYSTEMIC automatic software hardening solution**
  - **Reminder:**
    - **Painless** software security by binary file changes. **Effortless** at development, **Infra and packaging agnostic deployment**
    - Security menu: Self-authentication before start, Confidentiality preservation, Integrity preservation, execution control (DRM, machine binding), Fingerprinting-instance tracking
  - **Disruptive paths developed in INSPIRE-5Gplus project: (patent pending)**
    - Automated and SGX protected **runtime regulation** of protection power (and associated overhead).
      - “Always Systainable Software Security” publication at SecSoft workshop, NetSoft IEEE conference Miano 2022
    - **Software zoning** concept
      - Enforcing data (in clear) and software are only present **HERE ONLY**
      - Oppose to perennial IP spoofing-based node impersonation attacks
      - Data Zoning can be established leveraging software zoning and technically proven.
    - **Deep runtime monitoring** confering unambiguous and anchored evidences as: “the code trully executes now”, “at this location”, “in the normal expected flow” and “is integrated”

Thank you for your attention!

Find us at www.inspire-5gplus.eu

Twitter: @inspire_5gplus

Acknowledgment:

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