RIGOUROUS

RIGOUROUS: secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

Zero-touch cognitive and secure management framework

Antonio Skarmeta

University of Murcia – Spain

https://rigourous.eu/

RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933

RIGOUROUS: secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

11 partners from 8 countries

Project start January 1st, 2023, for 36 months

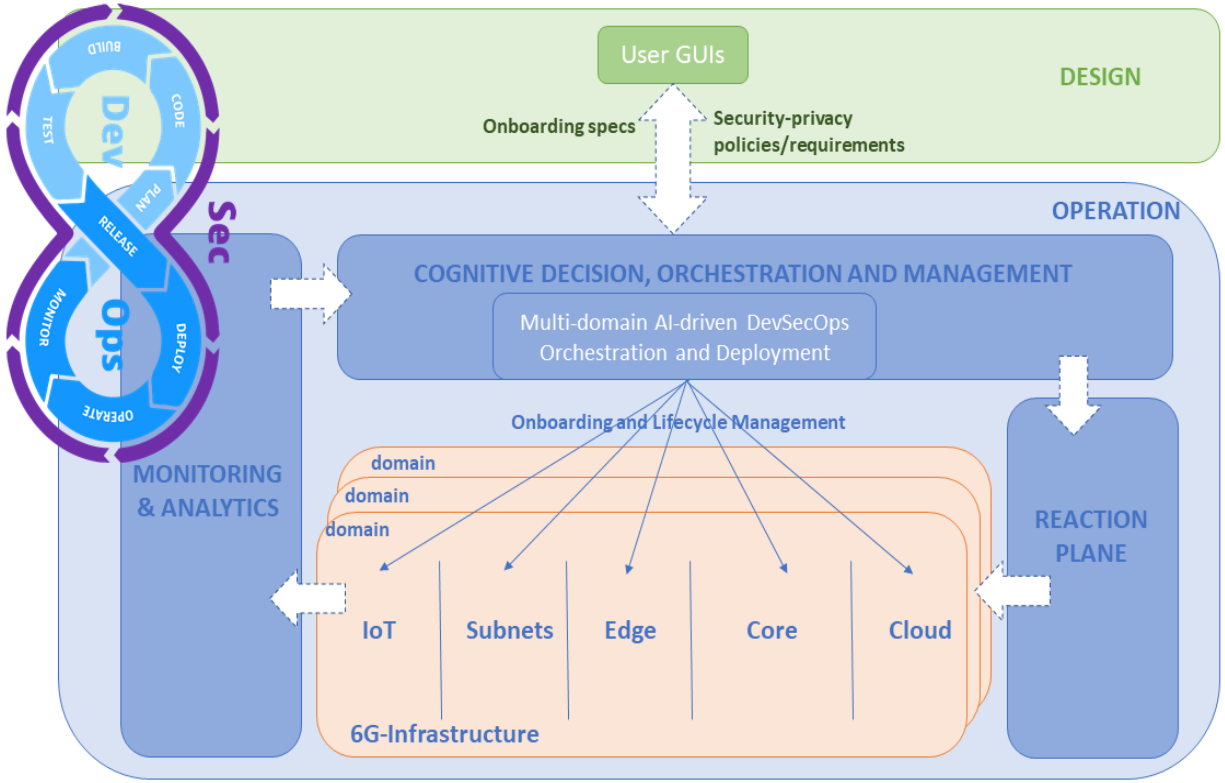
Total Cost 4 860 550€

Work programme topic addressed: STREAM-B-01-04 “Secure Service development and Smart Security”. HORIZON-JU-SNS-2022

1 (Coordinator)	University of Murcia (UNIV)*	UMU	Spain
2	ORANGE Romania*	ORO	Romania
3	LENOVO DEUTSCHLAND GMBH*	LNVO	Germany
4	RHEA System Luxembourg S.A. *	RHEA	Luxembourg
5	EBOS Technologies Ltd (SME)*	EBOS	Cyprus
6	WINGS (SME)*	WINGS	Greece
7	OneSource, Consultoria Informática Lda. (SME)*	ONE	Portugal
8	ICT-FI (SME) * *	ICT-FI	Finland
9	University of Oulu (UNIV)*	OULU	Finland
10	Instituto de Telecomunicações (UNIV)*	ITAV	Portugal
11	University of the West of Scotland (UNIV) *	UWS	UK

Introduction

RIGOUROUS will introduce a new holistic and smart service framework leveraging new machine learning (ML) and AI mechanisms, which can react dynamically to the ever-changing threat surface on all orchestration layers and network functions.



Smart service framework is capable of ensuring a **secure, trusted and privacy-preserving** environment for supporting the next generation of trustworthy continuum computing 6G services along the full **device-edge-cloud-continuum on heterogenous multi-domain networks**. This includes establishing compliance with the design of software (SW), protocols and procedures, as well as AI-governed mechanisms to cope with the security-related requirements in the **full DevOps lifecycle**, from the service onboarding up to the day-2 operations.

Objectives

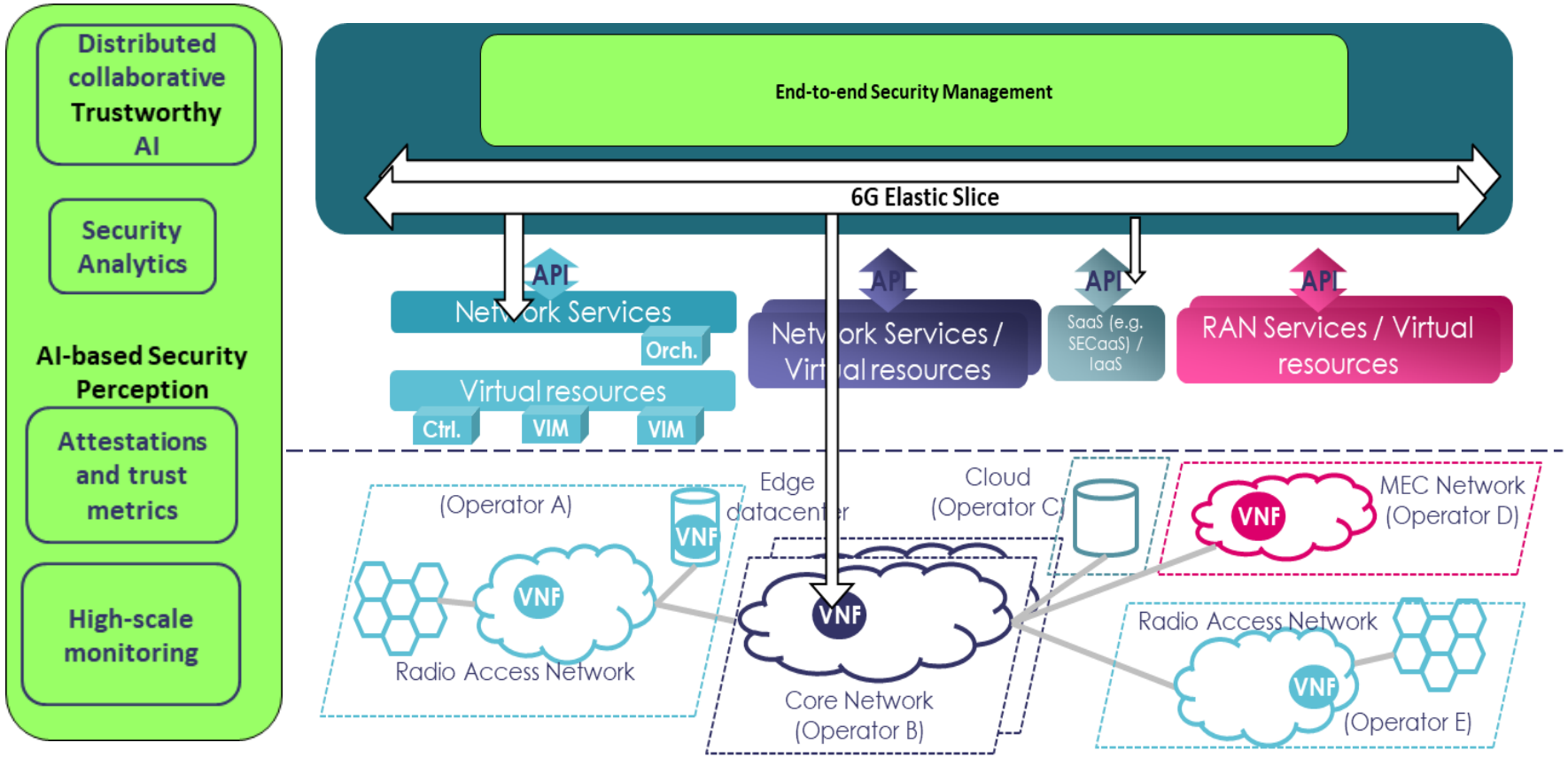
- O1: Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
- O2: Human-Centric DevSecOps
- O3: Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment
- O4: Advanced AI-driven Anomaly Detection, Decision and Mitigation Strategies
- O5: Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

Security Management architecture

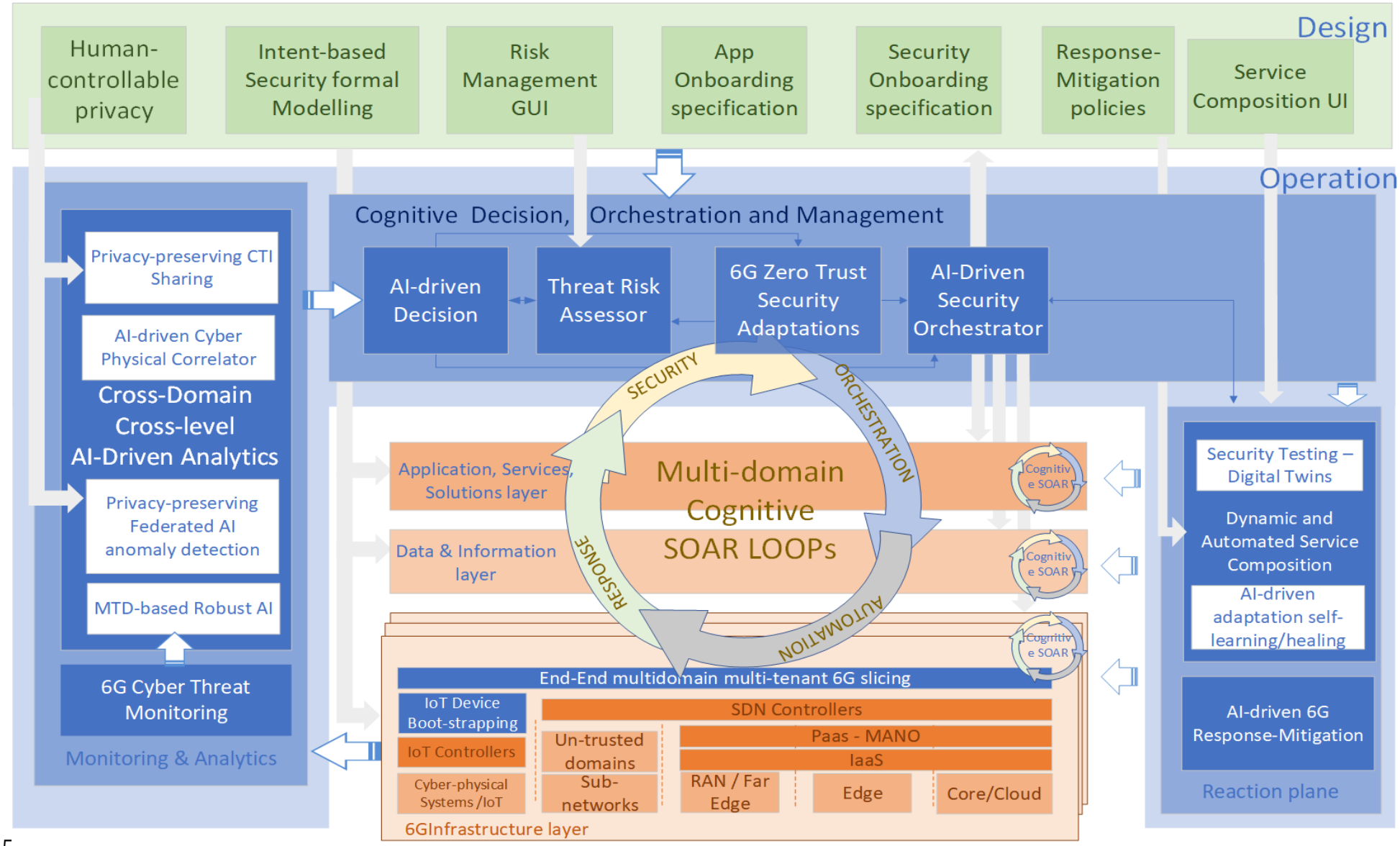
RIGOUROUS

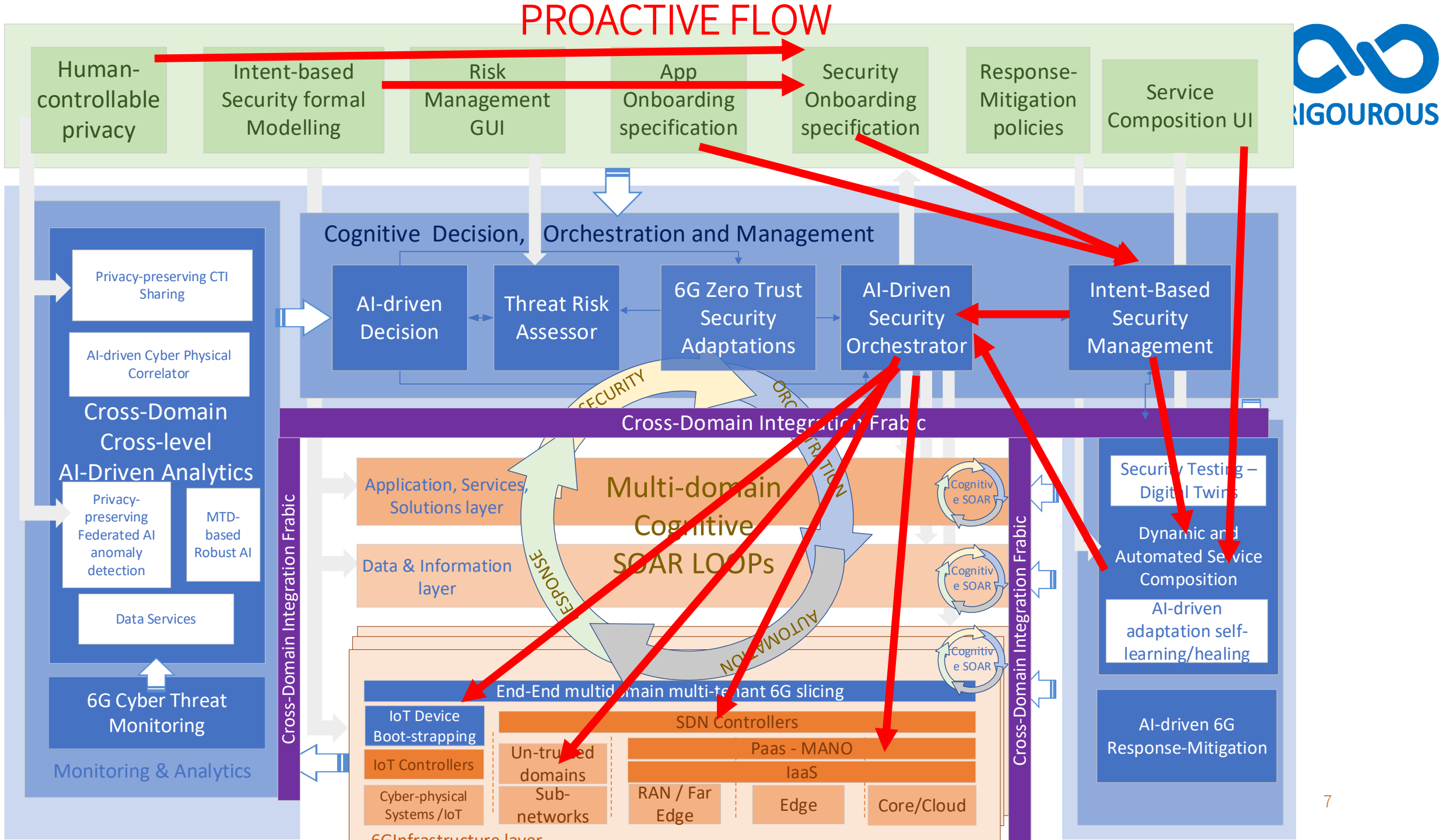
Challenges

- ZSM Security E2E orchestration
  - Adaptative and unattended cybersecurity
- Continuum of Trust
  - Trustworthy & privacy-preserving data mamagement
- Cross domain high-scale monitoring
  - Collaborative AI predictive análisis and mitigation
- Extreme virtualization and softwarization
  - **softwarization and cloudization based security solutions**
- ZTA Zero Trust Architectures
  - DLT-based trustworthiness

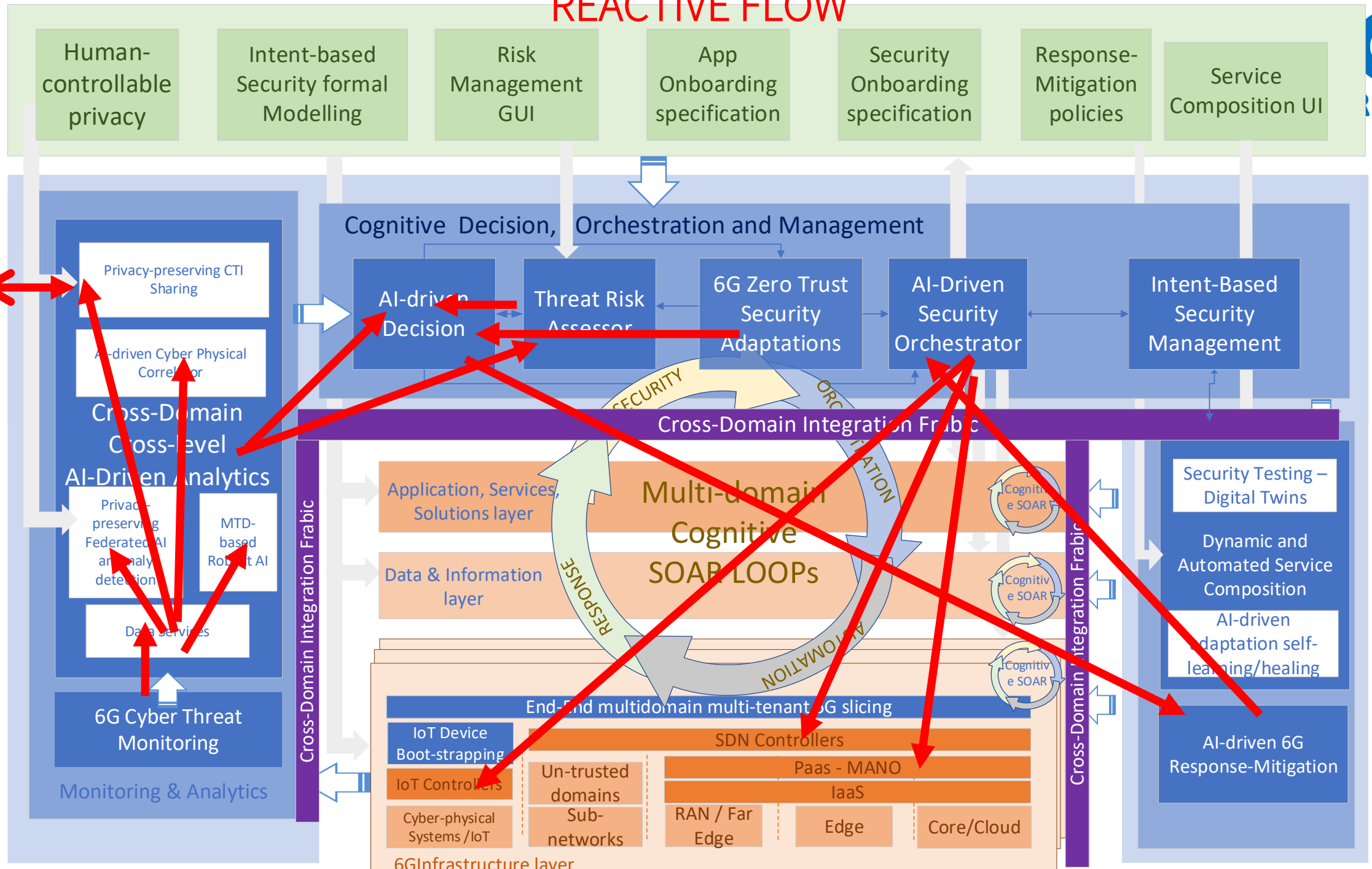


High-level Functional Architecture

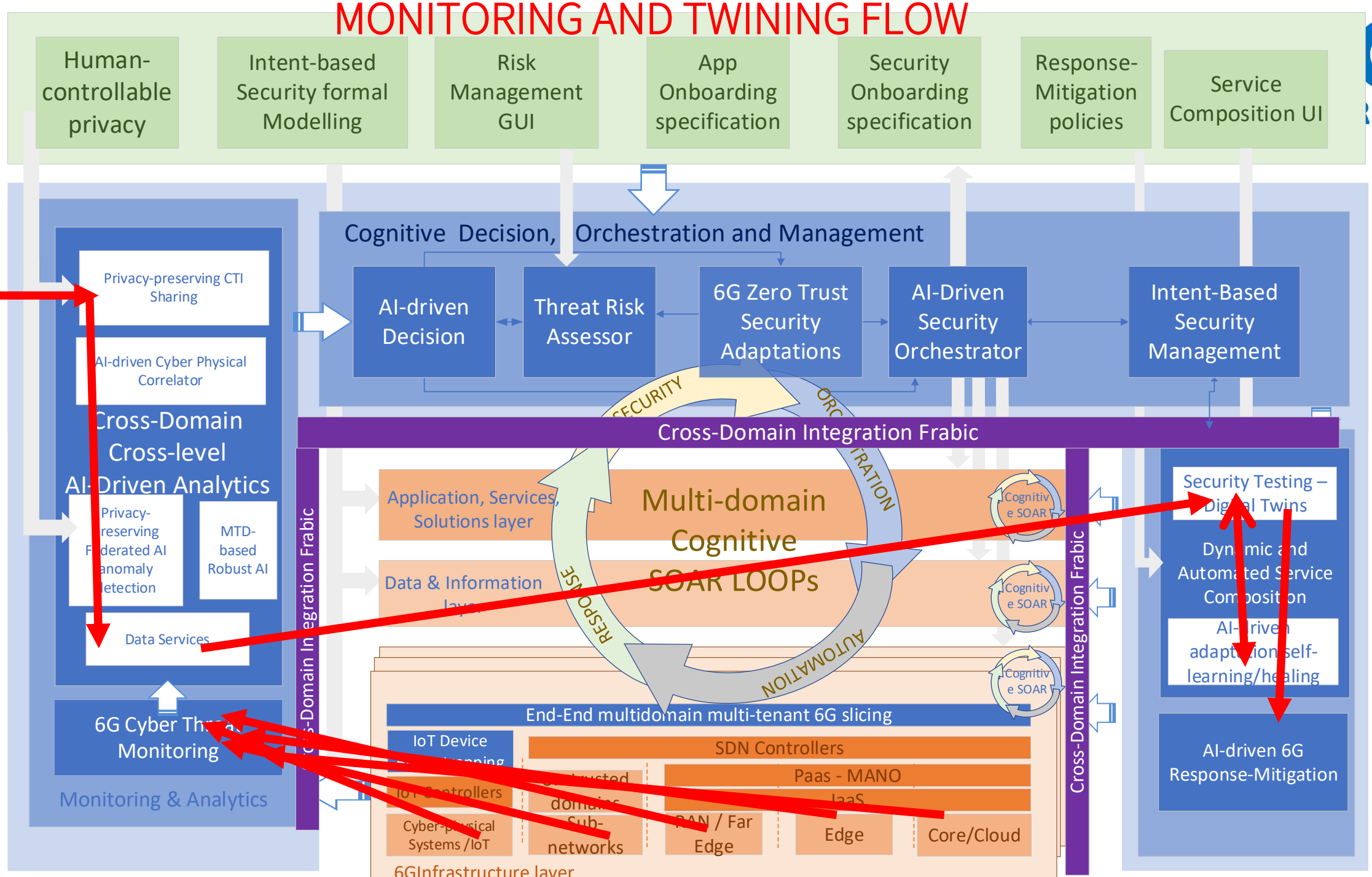



PROACTIVE FLOW
Human-controllable privacy
Intent-based Security formal Modelling
Risk Management GUI
App Onboarding specification
Security Onboarding specification
Response-Mitigation policies
Service Composition UI
Cognitive Decision, Orchestration and Management
AI-driven Decision
Threat Risk Assessor
6G Zero Trust Security Adaptations
AI-Driven Security Orchestrator
Intent-Based Security Management
Privacy-preserving CTI Sharing
AI-driven Cyber Physical Correlator
Cross-Domain Cross-level AI-Driven Analytics
Privacy-preserving Federated AI anomaly detection
MTD-based Robust AI
Data Services
6G Cyber Threat Monitoring
Monitoring & Analytics
Cross-Domain Integration Frabic
Application, Services, Solutions layer
Data & Information layer
Multi-domain Cognitive SOAR LOOPs
Cognitive SOAR
Cognitive SOAR
Cognitive SOAR
Cross-Domain Integration Frabic
Security Testing – Digital Twins
Dynamic and Automated Service Composition
AI-driven adaptation self-learning/healing
AI-driven 6G Response-Mitigation
End-End multi-domain multi-tenant 6G slicing
IoT Device Boot-strapping
IoT Controllers
Cyber-physical Systems /IoT
SDN Controllers
Paas - MANO
IaaS
Un-trusted domains
Sub-networks
RAN / Far Edge
Edge
Core/Cloud
6GInfrastructure layer

REACTIVE FLOW

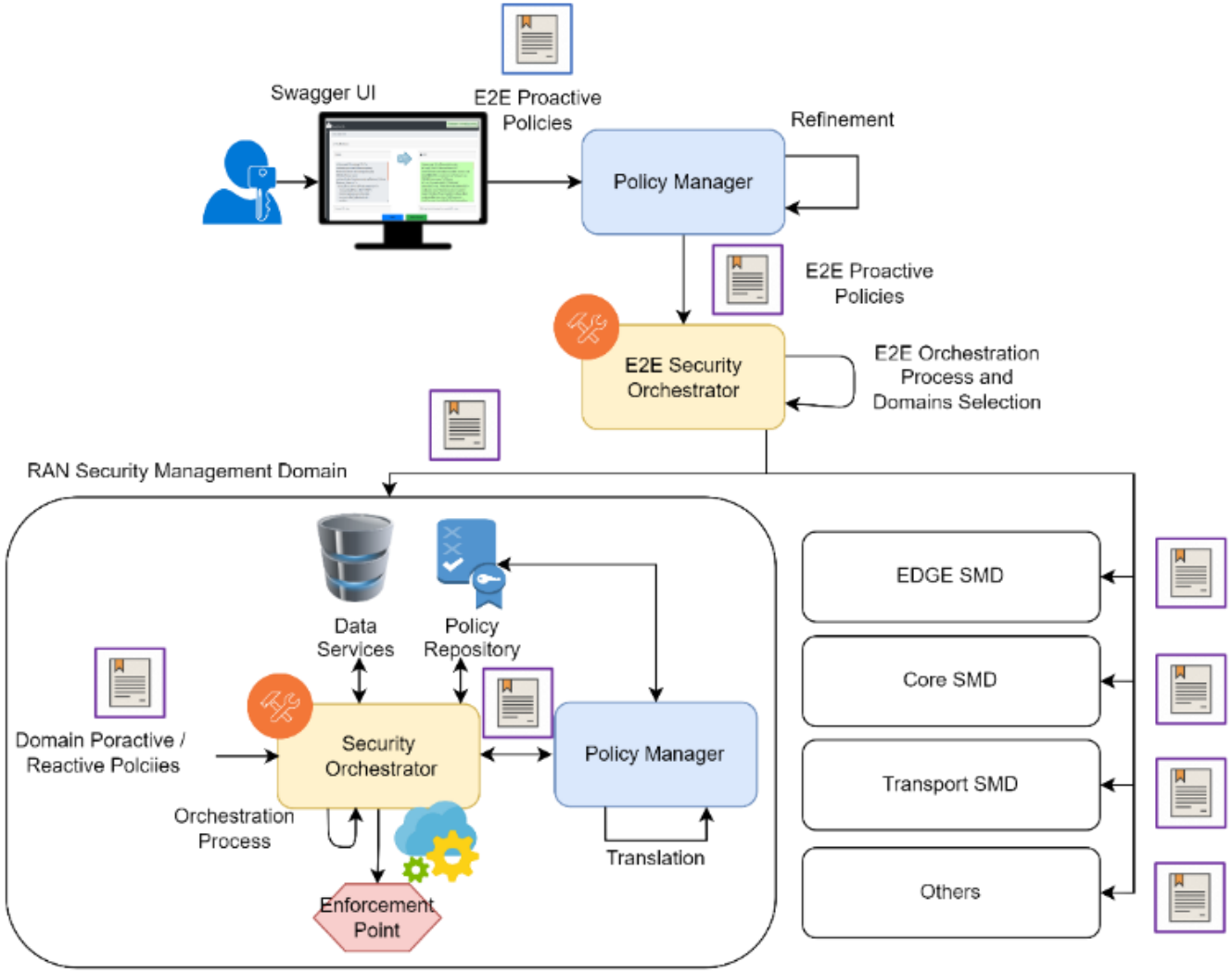


MONITORING AND TWINING FLOW



Policy-based AI-driven Security orchestration

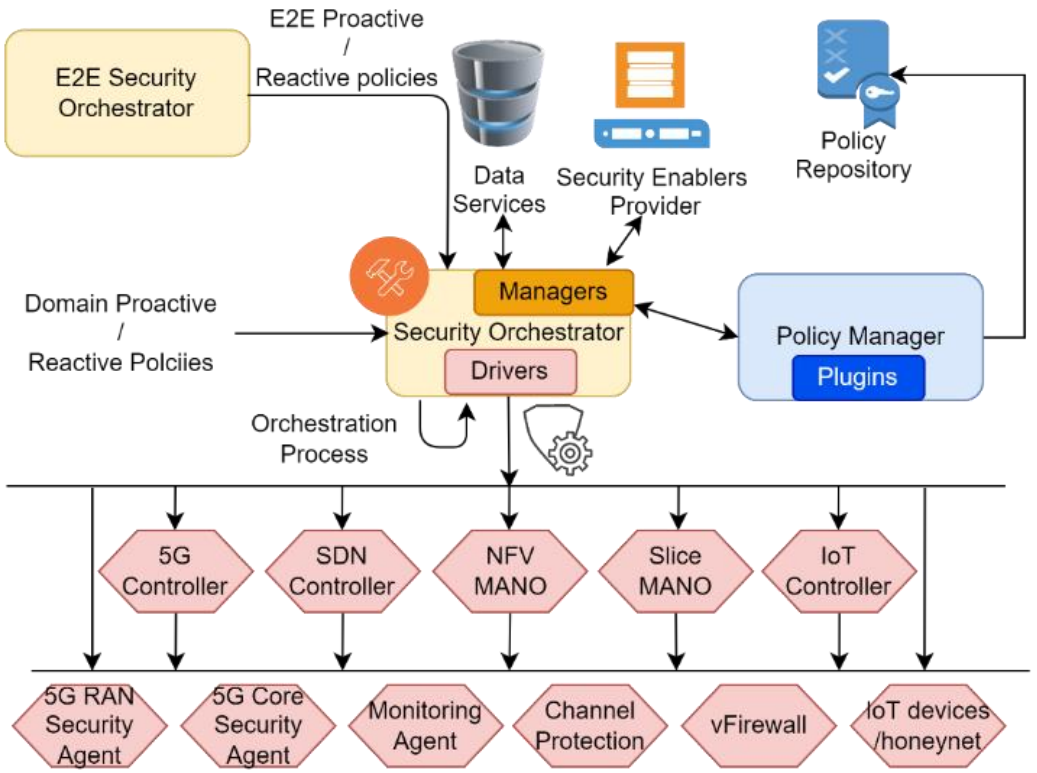
- User intent driven security policy definition
- The orchestrator will be driven by AI to make their chaining and orchestration decision
- Rely on special modules to translate the intents, policies and behavioural profiles coming from the decision into concrete actions
- Federated Learning (FL) approach to make orchestration decisions
- Decide best actions for dynamic provisioning, deployment, and reconfiguration (during operation) of the virtual network security functions and associated intents and policies
- Orchestrator will consider the time- and space-varying parameters of the network, such QoS capacities, actual resources constraints (CPU, RAM, storage), system status, current deployed policies, and threat incidents…



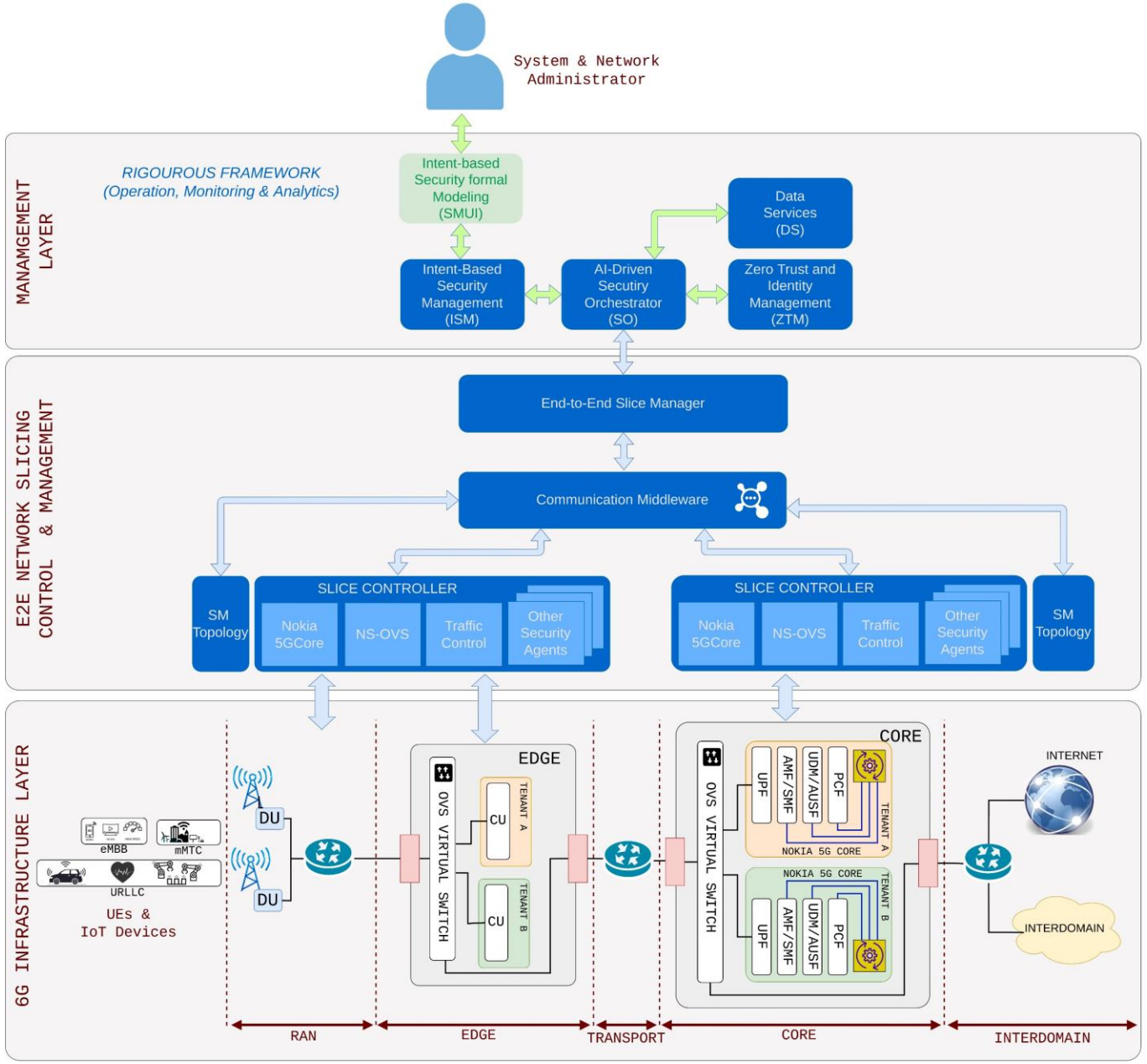
Policy-based AI-driven Security orchestration

- Extensible orchestration enforcement:
  - NFV, SDN, IoT Controllers
- Integration with Security Enabler Providers (to enforce actions) and Trust Managers to make decisions
- ETSI ZSM approach

- KPIs
- **KPI-5:** +10% increased accuracy in orchestration.
- **KPI-6:** AI-powered Orchestration of four (04) kinds of resources, namely: services, devices, virtual network functions, and physical network functions
- **KPI-7:** Orchestration of resources in four (04) kinds of horizontal network segments, namely: IoT, RAN, Edge, Core-Cloud
- **KPI-8**: Number of AI Algorithms devised for 6G orchestration >3



E2E Network and Security Slicing



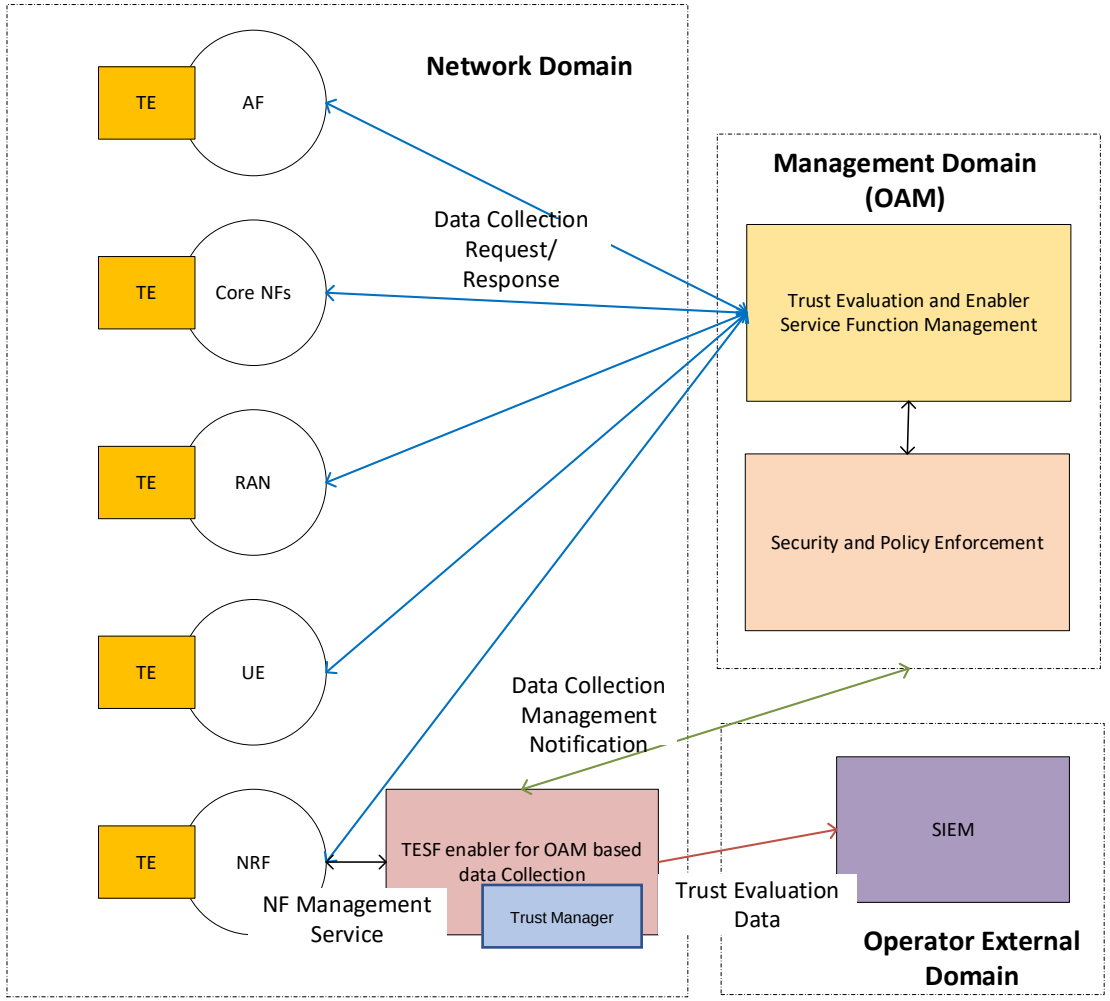
- Integration of WP3 components towards a E2E Network Slicing control and management framework.

- Security Policies (SPs) and Security Level Agreements (SSLAs) enforced in the data plane as Network Slices.

SPs/SSLAs → E2E Multi-domain Mult-tenant Network Slices

- Covering all network segments (RAN, Edge, Core, Transport, …) in a technology agnostic manner
- <u>Security Slicing:</u>
- Security slice composed of set of security policies.
- Automatic set-up of multidomain security channels associated to a security slice. e.g. Ip-Sec

Trust Evaluation and Enabler Service Function Management



Goals

The Trust Evaluation and Enabler Service Function Management and TESF enabler are components to be introduced to the current architecture which

- can consume data from the network entities (e.g., UE/RAN/NFs) about the abnormal behaviours

- further to be analyzed and assign trust scores.

Requirements

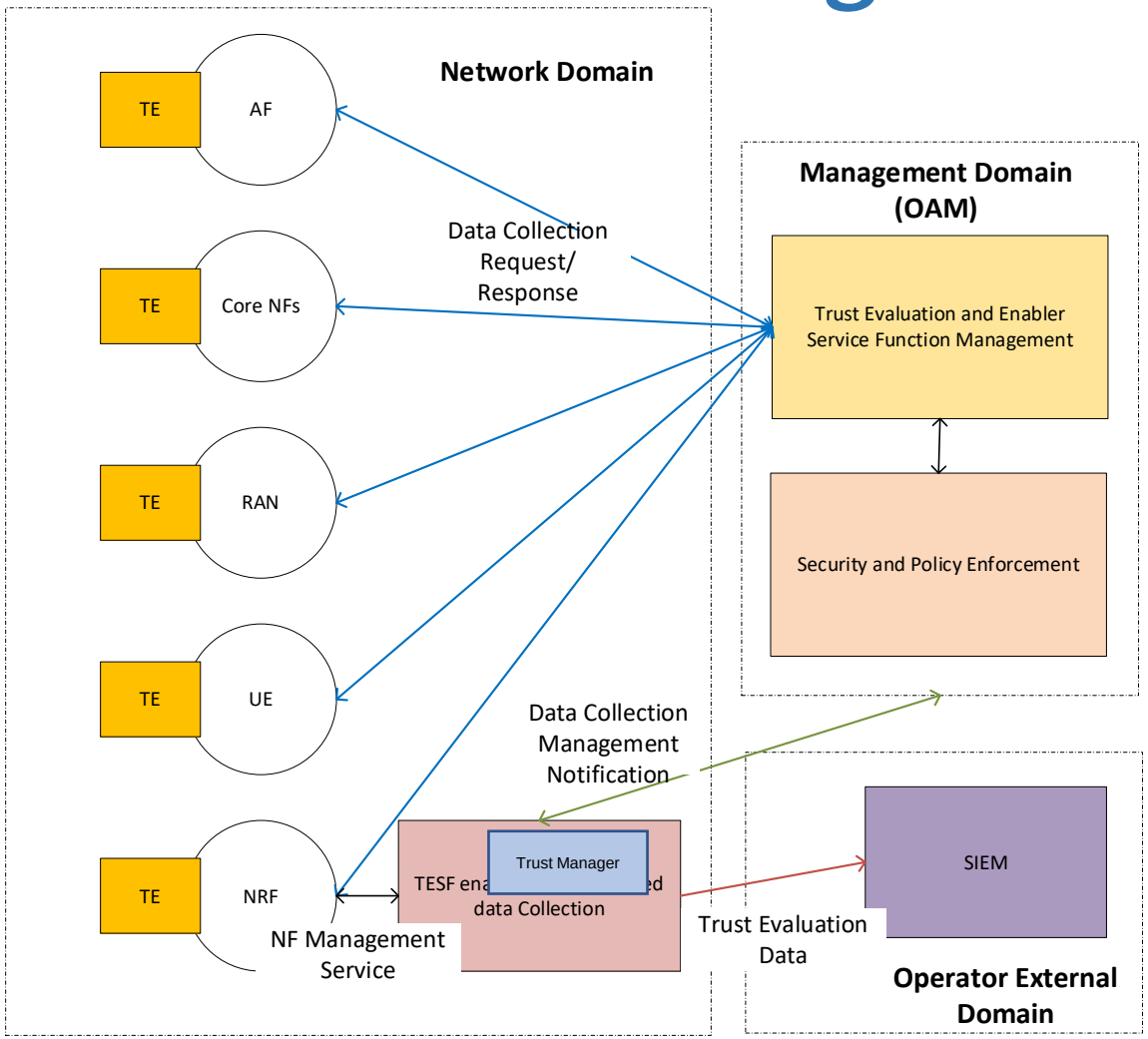
E.g., NFs in the Core network can expose abnormal behaviour related data through APIs, or their data can be collected by the OAM and TESF enabler (e.g., can be an NWDAF instance)

Synchronized notifications services to be developed for data collection and management through the TESF enabler.

Targeted Data Collection

NF resource usage
NF resource configuration
Violations of specified normal behaviors
Service requests exceeding configured limits
Critical configuration changes

Trust Evaluation and Enabler Service Function Management



Functionalities

The Trust Enablers in the network functions/ entities are the enablers for the end points of data collection.

The data is collected through either the management domain or directly to the TESF using Data Collection Request/ Response service(s).

The data collected are evaluated using the SIEM by providing via Trust Evaluation Data Interface.

The Trust Manager associated with the TESF performs trust score evaluation and informs the NRF through NF management service and Security and Policy Enforcement Block (or the security Orchestrator) through Data Collection Management Notification.

Targeted Data Collection

NF resource usage
NF resource configuration
Violations of specified normal behaviors
Service requests exceeding configured limits
Critical configuration changes

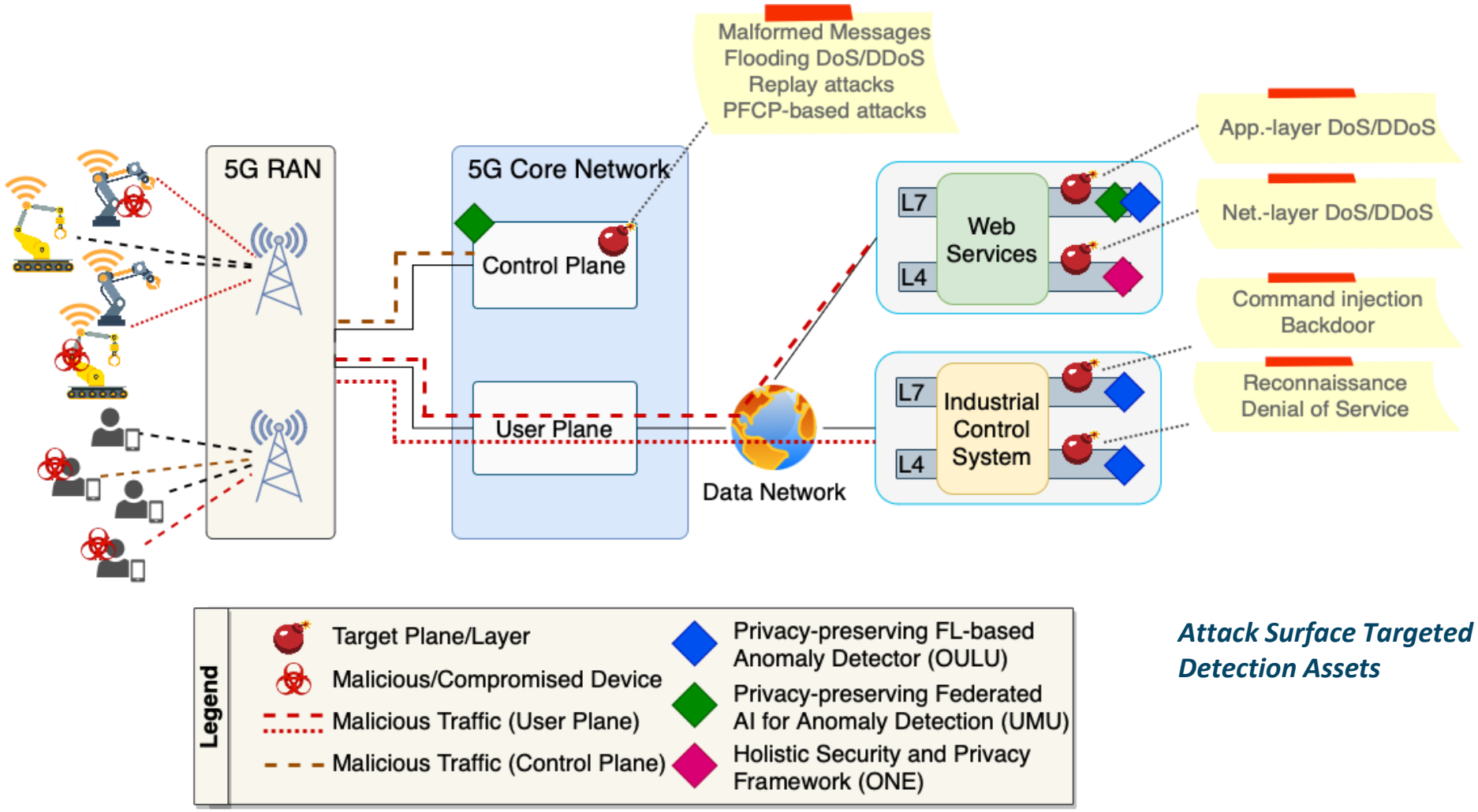
NFV Privacy Aware Onboarding Specification

- Policy driven approach for privacy modelling.
- **Privacy-quantifier** considers the service and NFV descriptions, as well as other input from users and metadata, to compute the privacy impact of an entity
  - Performs analysis executed over the application and/or its description and provides a privacy related score. Depending on the application, and the developer's approach, two sources are considered for this score: developer provided information, and automatically assessed information.
- Two methods
  - the developer specifically stating the data processing characteristics of the application, including which data is processed, which data is stored and how, and which data is communicated with specific external endpoints. These endpoints relate to external services on a Service Cloud.
  - A tools estimates how data is processed/stored and which is the connectivity graph with external endpoints. both methods result in a quantification and composite score.
- The proposed architecture accommodates service updates.
  - It establishes a control version to maintain a privacy benchmark as the service evolves.
- The privacy quantification component is utilized to re-evaluate the privacy level of the updated service, thereby updating the final metric.
- This approach establishes a continuous cycle of privacy testing and monitoring (**DevPrivOps**).
  - Privacy quantification and **re-quantification** ensure ongoing assessment and refinement of the service's privacy practices.
  - This iterative approach promotes continual enhancement of privacy practices, aligning the service with evolving privacy standards and best practices.

AI-driven Security Evolving, Response and Mitigation

- Design and implementation of all the **enablers to achieve a fully functional close control loop** for automated security mitigation against cyber-attacks
- Novel **topology inventory** agent able to detect the most modern infrastructure with the main intention to gain situational awareness of the network topology
- **Novel intrusion detection systems** able to work in the envisioned 6G overlay networks and provide support to perform the detection of well-known cyber attacks
- Design and implementation of a **planner component** able to take topological decision about where to act in the network

AI driven federated cross-domain analytics

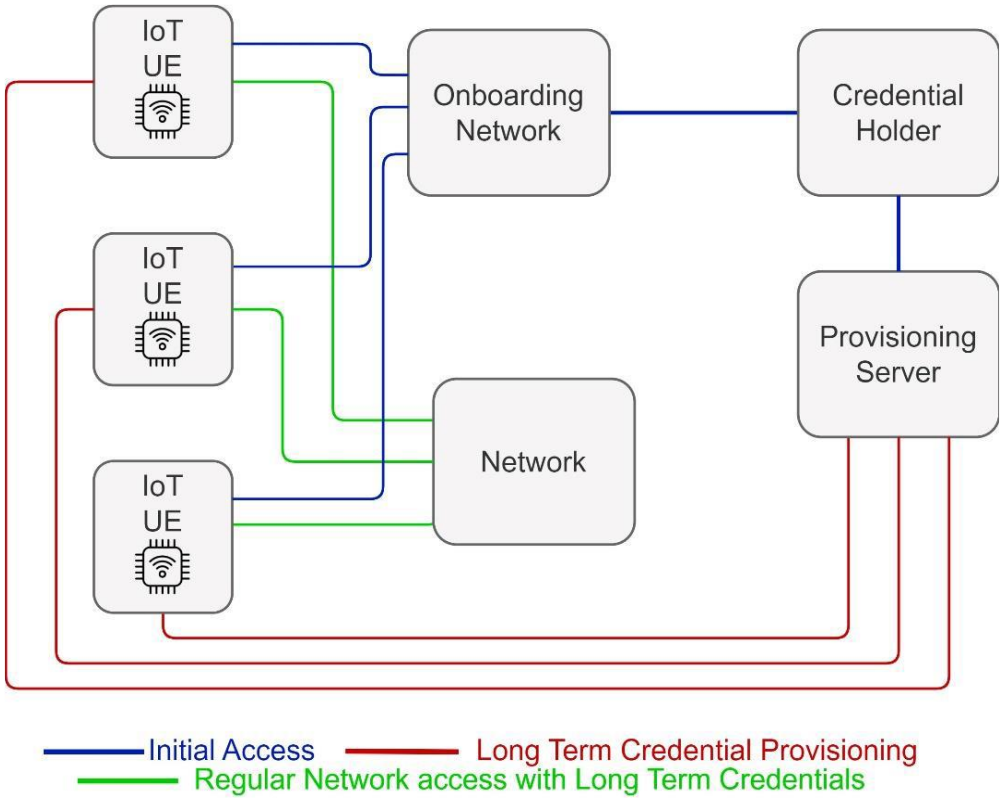


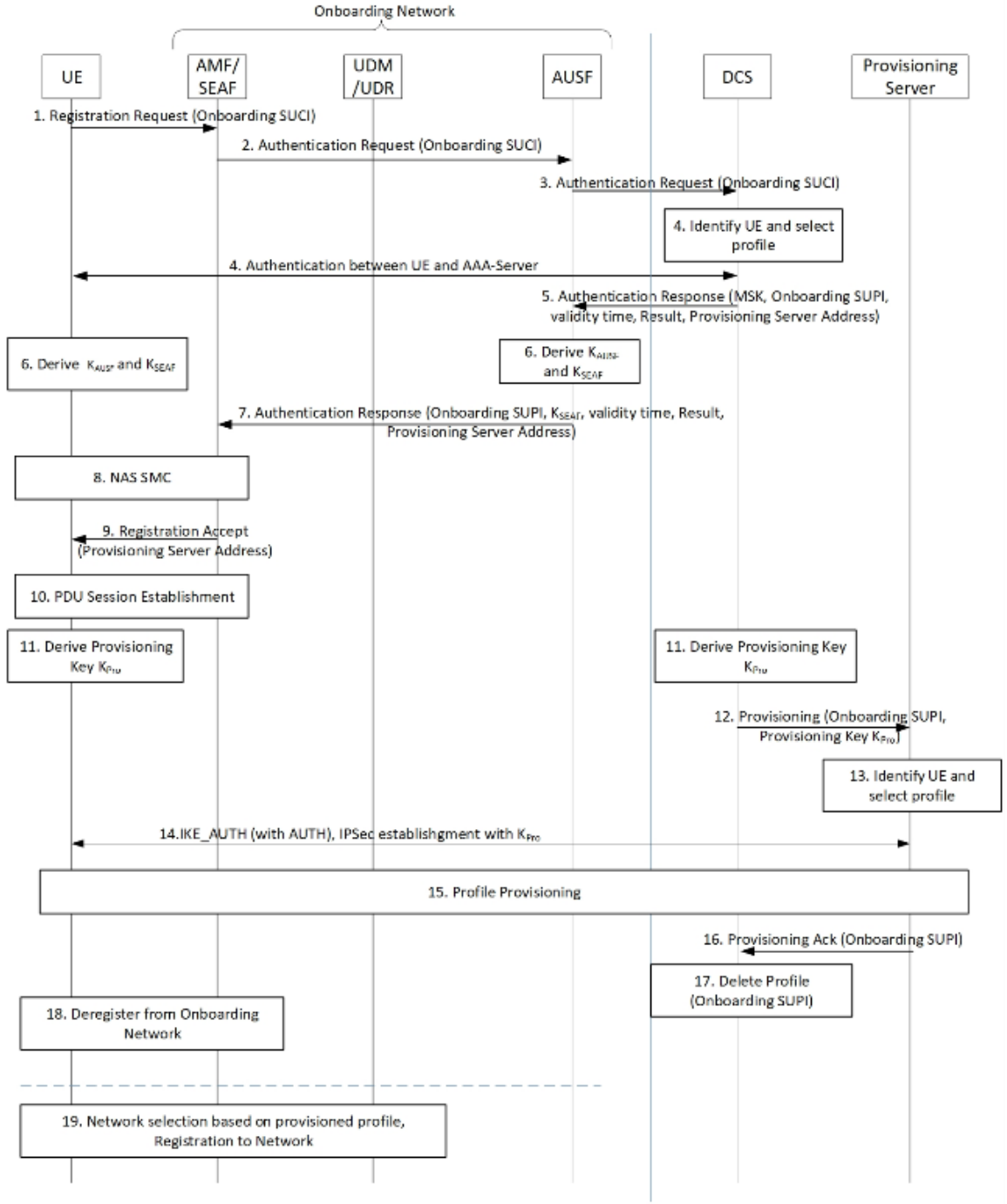
Attack Surface Targeted by RIGOUROUS Anomaly Detection Assets

Network self-protection enabler

- Network Self-Protection agent, a software data plane enabler to fulfil the RIGOUROUS requirements regarding network data-path slicing capabilities:
- Enhanced programmability of the data plane allowing the enforcement of advanced Security Policies dynamically in real time.
- Support for the enforcement of fine-grained network slicing in overlay networks with different levels of nested encapsulation.
- Support for network protocols widely adopted in mobile and multi-tenant virtualised deployments such as GTP, VXLAN, GRE or GENEVE used to provide user mobility and tenant traffic isolation.
- Scalability levels to cope with a large number of users simultaneously connected to the infrastructure.
- OpenVSwitch (OVS) has been selected as the baseline for the implementation of the Network Self Protection with the following extensions:
    - Thee OVS data structures and Open Flow tables with new fields matching the new flow data extracted by the novel 6G traffic classifier.
    - Open Flow protocol extension to allow control and management layers a flexible and fine-grained definition of flows. That is, enabling a fine-grained specification of network flows attached to a network slice.

Bootstrapping

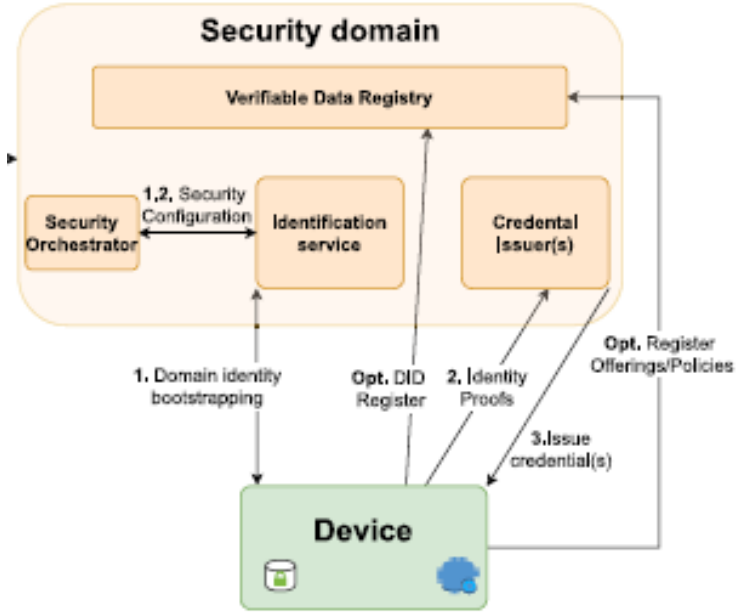


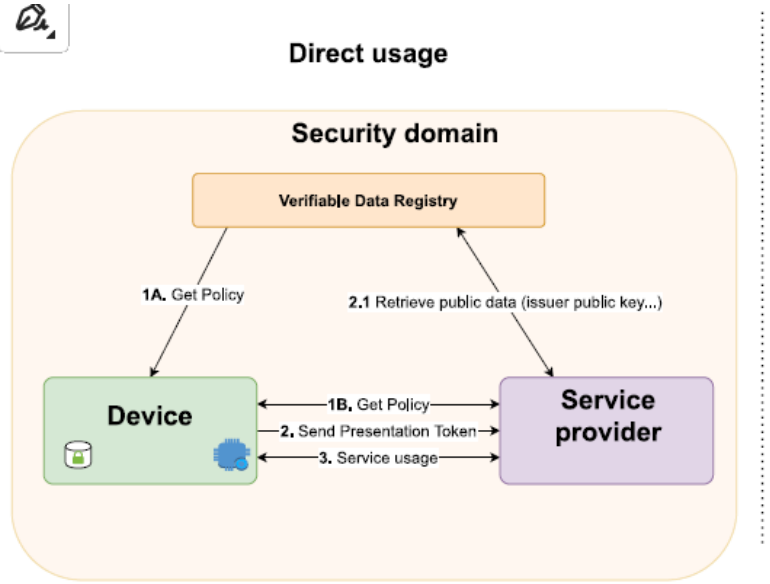


Bootstrapping and enrolment leveraging pp-ABC system

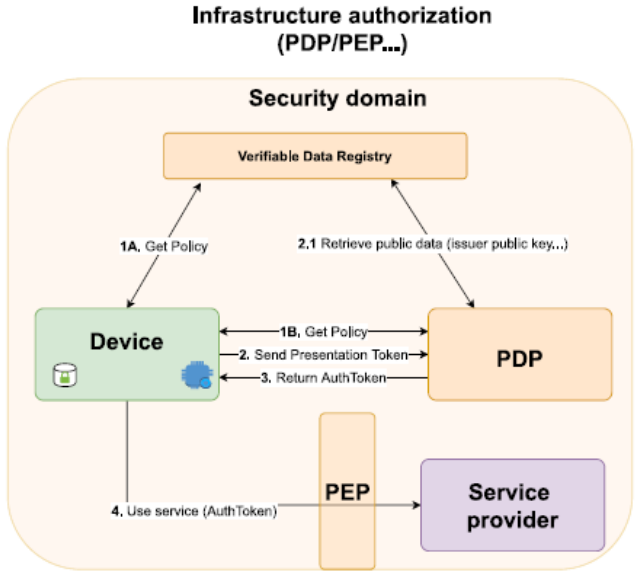
- Privacy-preserving ABC scheme for verifiable credentials
- Compatible with LNVO proposal
- Zero knowledge proofs for presentation
- Possible integration with DLT

Verifiable Credential-provisioning



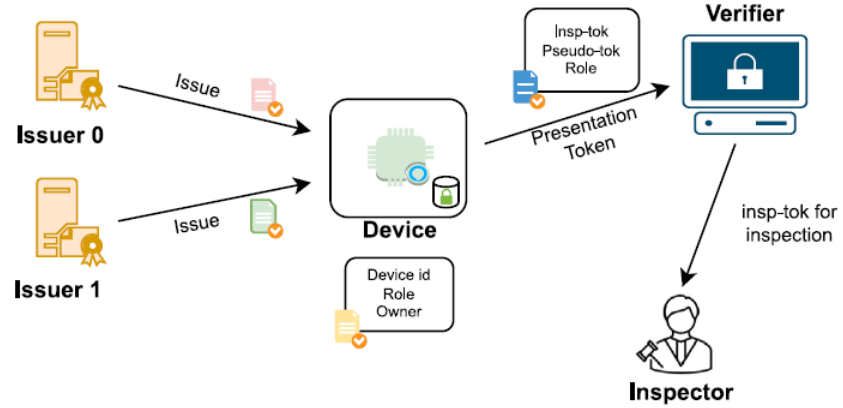


(a) Direct communication



(b) Authorization infrastructure

Credential presentation



25/01/2024

RIGOUROUS: secu**R**e des**IG**n and depl**O**yment of tr**U**sthwo**R**thy c**O**ntin**U**um computing 6G **S**ervices

Thanks

Follow us at https://rigourous.eu/

Antonio Skarmeta skarmeta@um.es

University of Murcia - Spain

23/02/2023

RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933