Intelligent Security and Pervasive Trust for 5G and Beyond

Akis Kourtis, PhD
NCSR “Demokritos”

Infocom Virtual Event 2020

INSPIRE-5Gplus at a Glance

INSPIRE-5Gplus

Research Programme

Horizon 2020 / 5G PPP
ICT-20-2019-2020

Duration

36 months / Nov 2019 – Oct 2022

Total Budget

5.99 million euro

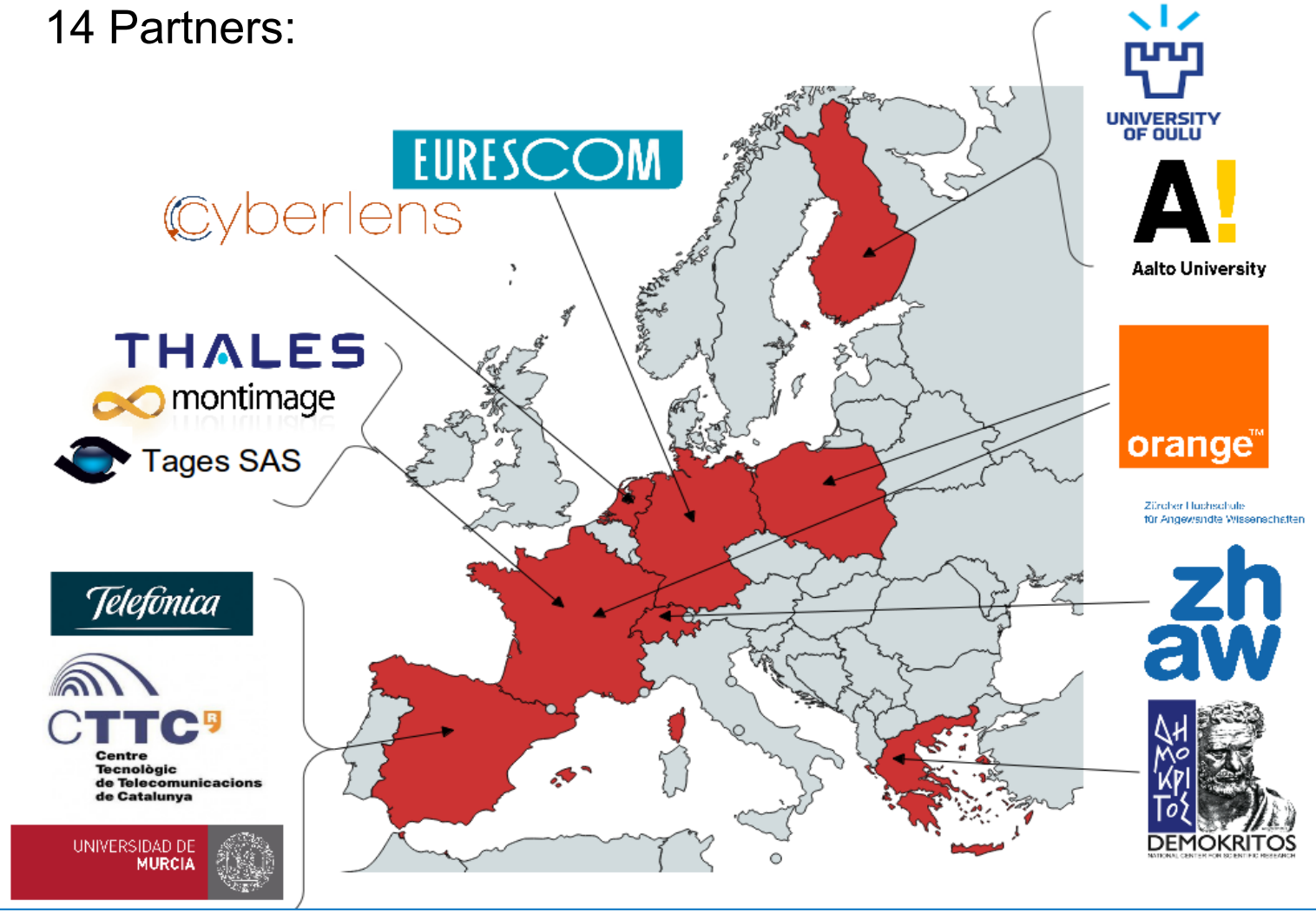
Project Coordinator

Eurescom, Germany

Technical Manager

Thales, France

14 Partners:



INSPIRE-5Gplus Vision for 5G and beyond security

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.
- Promote technical and/or societal innovation based on results achieved

INSPIRE-5Gplus – Objectives

INSPIRE-5Gplus

- Objective I “Establish architecture requirements, enablers and use-case”
  - Significantly advance 5G and Beyond Security embracing all anticipated changes whereas focusing on most pressing 5G security needs called by Platforms and/or Verticals as well as necessary evolvement of the security architecture.
- Objective II “Assess 5G security”
  - Perform a thorough assessment of 5G security situation in view of key concerns and identify 5G security solutions (assets) to date vs to come (develop) to meet the needs to achieve 5G & Beyond Security Vision
- Objective III “Develop advanced security services”
  - Develop intelligent and autonomous end-to-end cyber security services to be integrated in the 5G network graph with the aim of predicting, detecting and mitigating the impact of current and upcoming threats targeting next-generation networks and leveraging on existing tools, techniques and concepts but also (fully) embracing new ones (e.g., AI and ML, TEE, DTM, ZSM, Liability concepts, blockchain and DLT).

INSPIRE-5Gplus – Objectives (cont.)

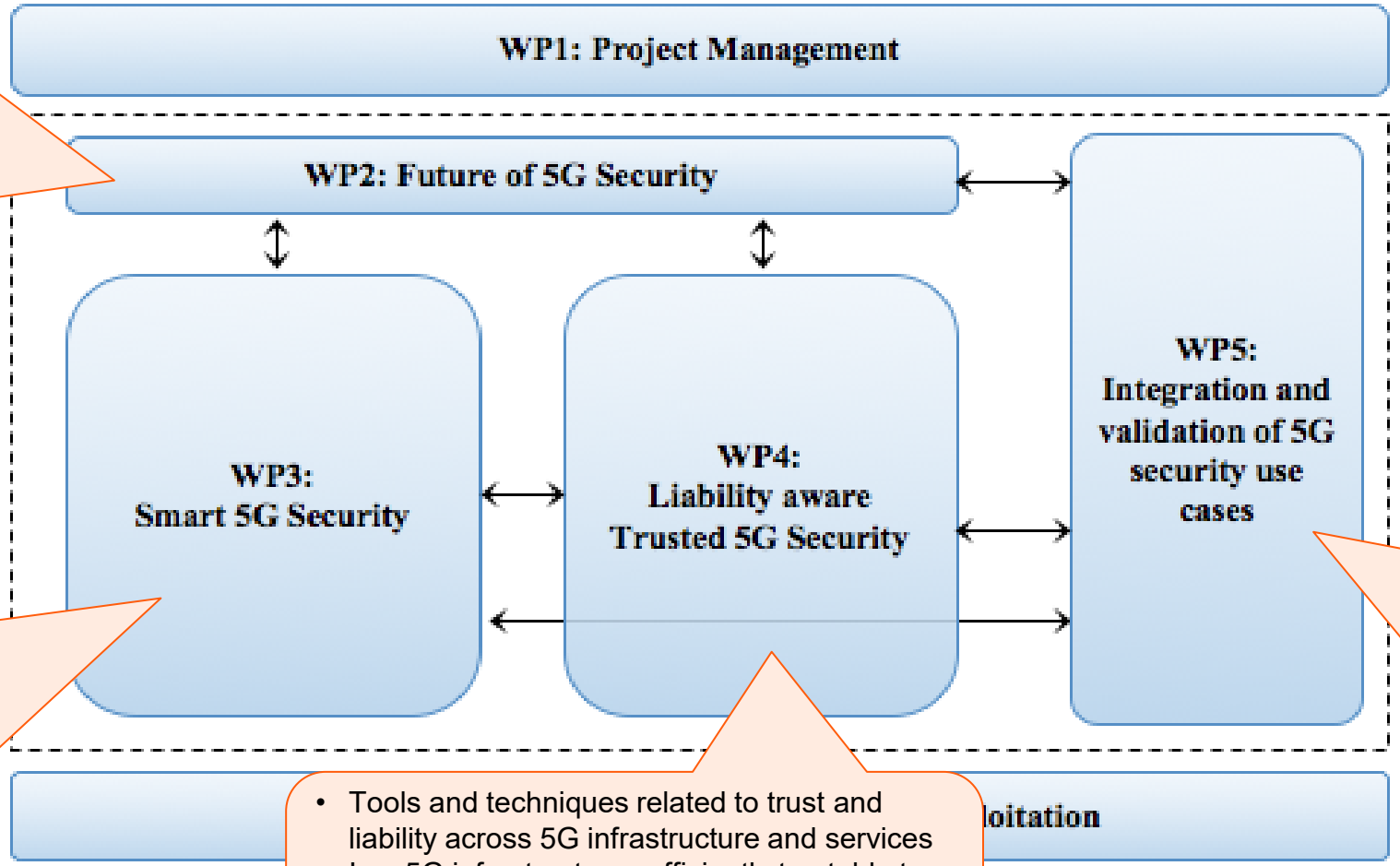
INSPIRE-5Gplus

- Objective IV “Enhance trust management”:
  - To deliver novel mechanisms to foster and manage trust and liability in 5G and beyond networks, supporting confidence between parties and compliance with regulation.
- Objective V “Demonstrate INSPIRE-5Gplus innovation potential”:
  - Demonstrate the innovation potential of some of the carefully selected security assets in the context of the platforms and verticals represented within the consortium with support of the projects attached and/or interested to adopt and make these demos happen.
- Objective VI “Create a lasting impact”
  - Create lasting impact, acting as a consensus builder on aspects relevant to security of 5G and beyond.

Organisation of project activities

INSPIRE-5Gplus

- New architecture for empowering **zero-touch E2E smart** 5G and beyond sec.
- Def. advanced security use cases, exemplifying security, trust and liability challenges at platform and/or vertical level.



- Provide and develop new breed of security enablers, leveraging on advanced techniques (e.g. AI/ML)
- Provide intelligent and autonomic end-to-end cyber security services, able to detect and mitigate both existing and new threats targeting 5G networks

- Tools and techniques related to trust and liability across 5G infrastructure and services
- Is a 5G infrastructure sufficiently trustable to operate critical services? (e.g. Industry 4.0)
- Provide evidence of Data protection, compliance with local regulation etc.

- Creation of an integration and experimentation framework, to validate certain 5G security use cases
- Based on the new and enhanced 5G security and trust / liability assets developed in WP3 and WP4

INSPIRE-5Gplus – Phasing approach

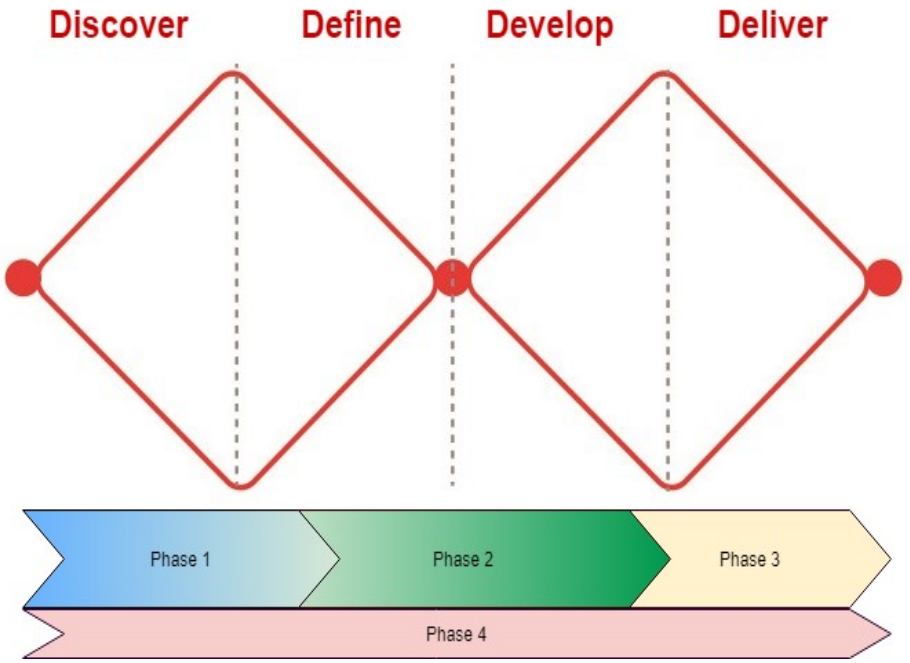
INSPIRE-5Gplus

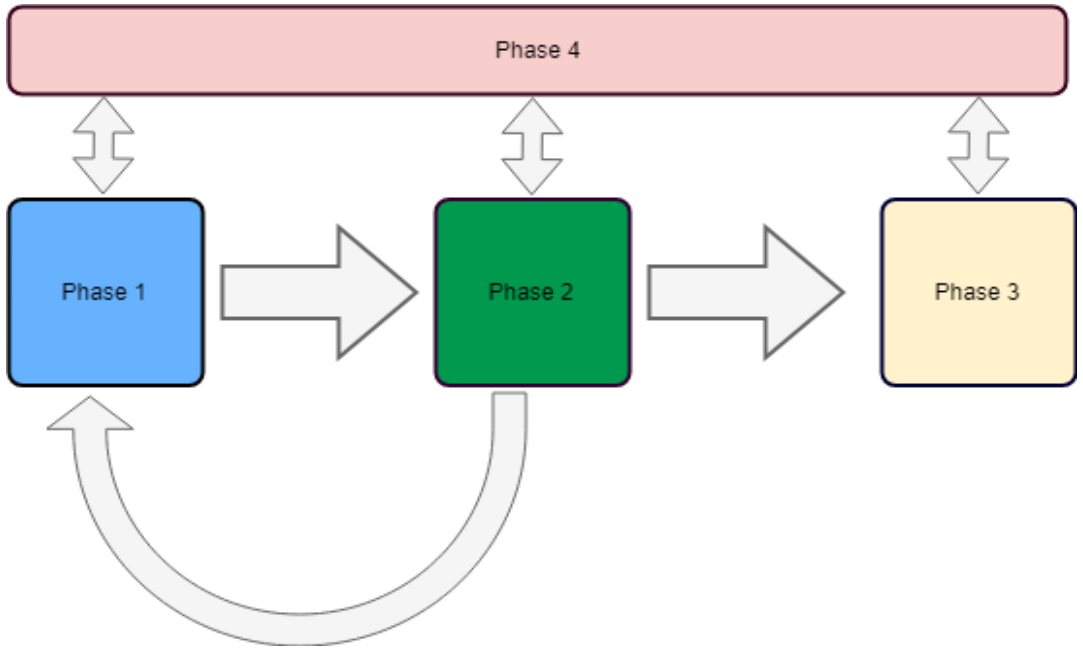
Phase 1: “Exploration of the current 5G security ecosystem (M1-M6)

Phase 2: “Progress Security of 5G systems to make it smarter, trustworthy but also more liable” (M7-M18)

Phase 3: “Integration and validation” (M19 to M36)

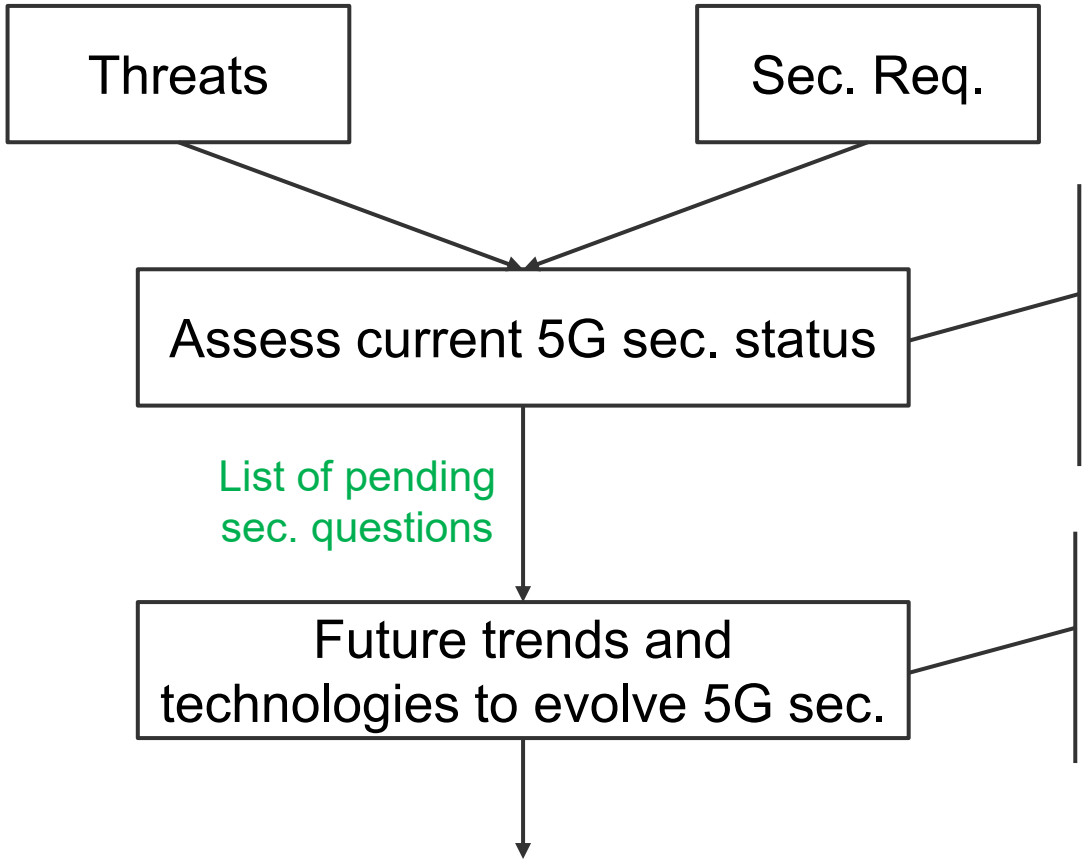
Phase 4: “Dissemination, standardization and exploitation” (M1-M36)





5G Security Evolvement Approach

INSPIRE-5Gplus



- Academic research SoTA
  - Infrastructure/Platform level
  - Management/Automation level
  - Service/Vertical level
- SDOs initiatives
- 5G-PPP projects
- Open source initiatives

- Automation & ZSM
- AI/ML
- Advanced sec. techniques (e.g., SSLA, cyber threat intelligence)
- Blockchain
- TEE
- Dynamic liability and RCA

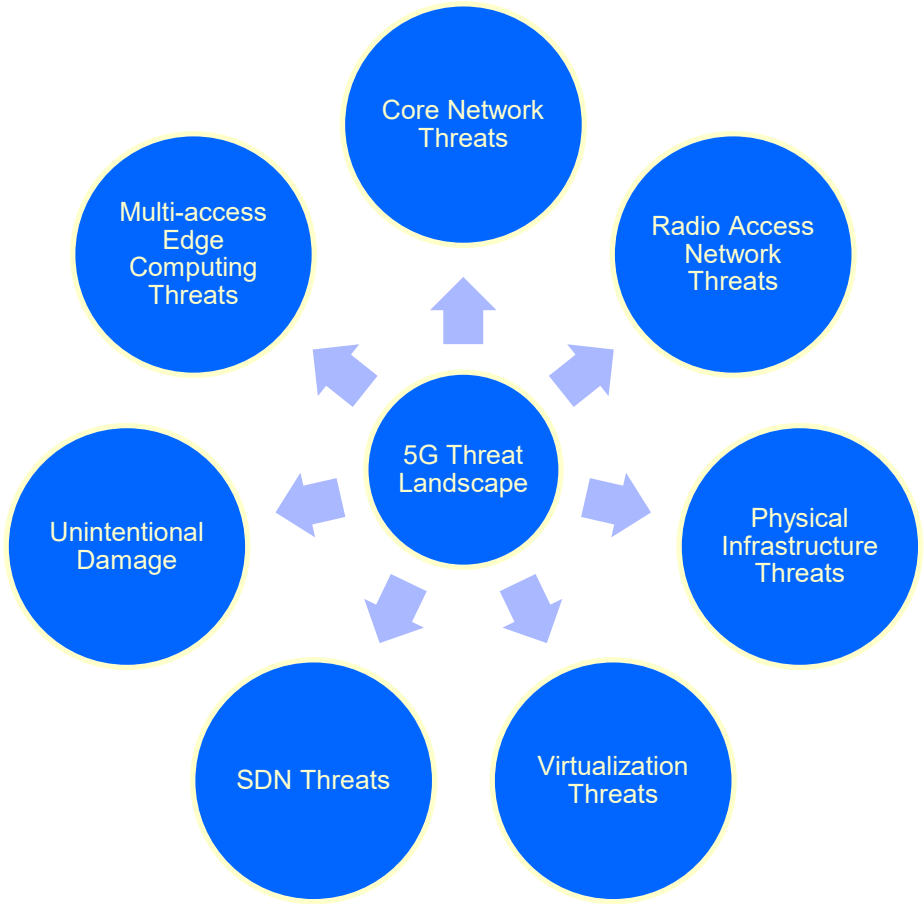
D2.1 – Outcome of the conducted study of the current situation and future trends of 5G security

(https://www.inspire-5gplus.eu/public-deliverables/)

5G (& Beyond) Security Threats & Requirements

INSPIRE-5Gplus

Threat type



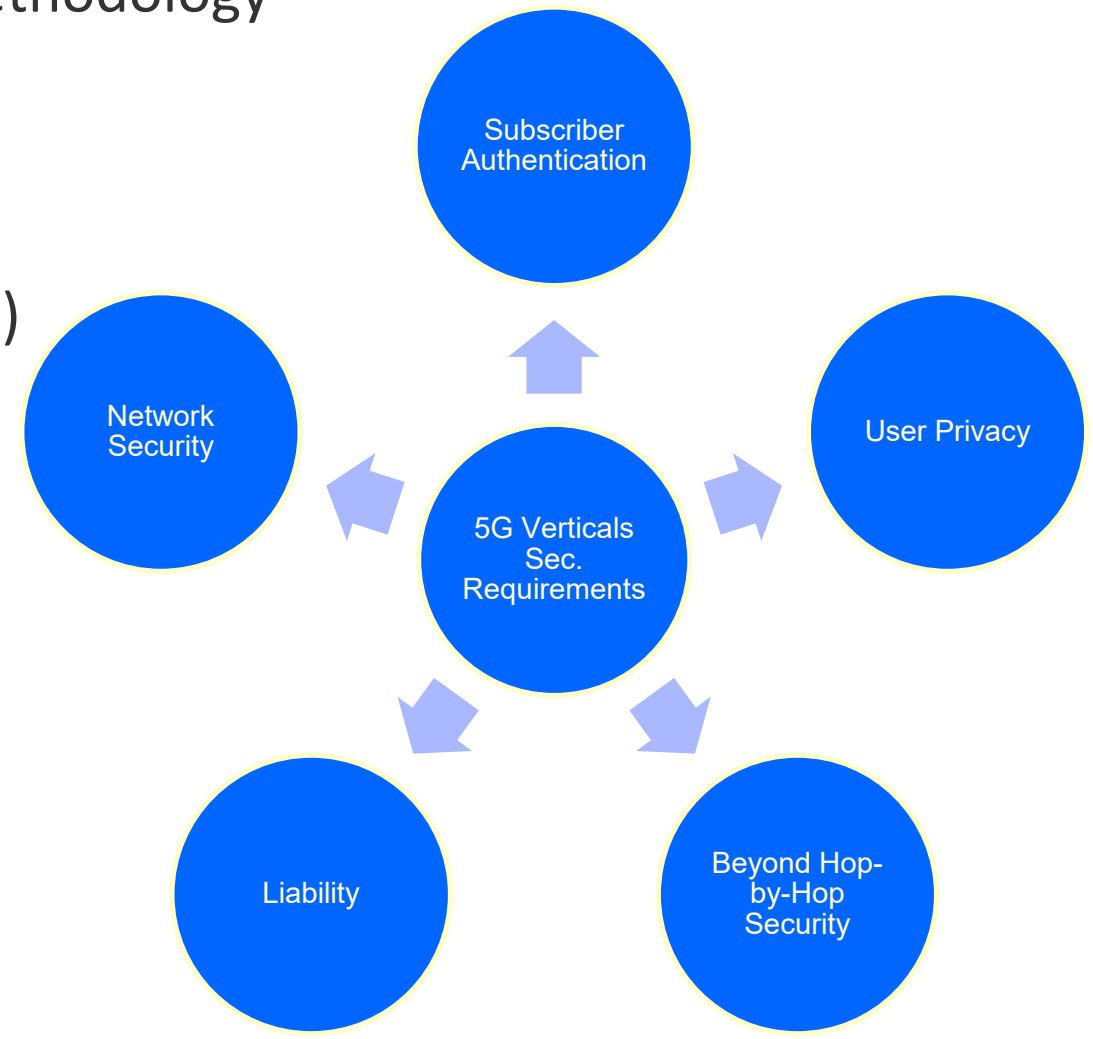
Threat Location

Based on "**Enisa Threat Landscape for 5G Networks"**. Nov. 2019

5G (& Beyond) Security Threats & Requirements

INSPIRE-5Gplus

- Security requirements identification methodology
  - Following NIST cybersecurity framework
  - Verticals oriented security analysis
- Four 5G vertical domains (Not exclusive)
  - Energy utilities;
  - Vehicular communications;
  - Enhanced content delivery; and
  - Media production and delivery.



5G (& Beyond) Security Threats & Requirements

INSPIRE-5Gplus

- Initial list of INSPIRE-5Gplus high-level security requirements

Security Requirement No.	Requirement
SEC-REQ-01	The 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system.
SEC-REQ-02	The 5G network shall only allow authenticated users to consume the services provided by the 5G system.
SEC-REQ-03	The 5G network shall warrant measurable level of availability of its services to the relevant stakeholders.
SEC-REQ-04	The 5G network shall ensure the necessary network capacity and network resources necessary for the critical operations of the 5G services.
SEC-REQ-05	The 5G network shall enable a secure platform for vertical services to be deployed.
SEC-REQ-06	The 5G network shall enable the state management of its platform components.
SEC-REQ-07	The 5G network shall be able to revert to previous states with minimal service disruption of deployed application in case of malicious compromise.
SEC-REQ-8	The 5G network's security mechanisms should not impact the functional requirements of critical operations for vertical applications.
SEC-REQ-9	The security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality.
SEC-REQ-10	The security mechanisms of the 5G network shall be able to measure/evaluate trust level of its components and platforms and share this information with verticals in a safe and trustable way.
SEC-REQ-11	The security mechanisms used in a complex 5G eco-system shall be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.
SEC-REQ-12	The 5G eco-system shall be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.
SEC-REQ-13	Technologies used to distribute over 5G eco-system (end to end) and evaluate post security incident root cause of failure are trustable.
SEC-REQ-14	The 5G system must provide security mechanisms to ensure that user (and endpoints) data are securely processed and stored wherever it is processed or stored. Both confidentiality and integrity guaranties shall be brought all along the full lifecycle of the data in transit, process and storage.

5G (& Beyond) Security Threats & Requirements

INSPIRE-5Gplus

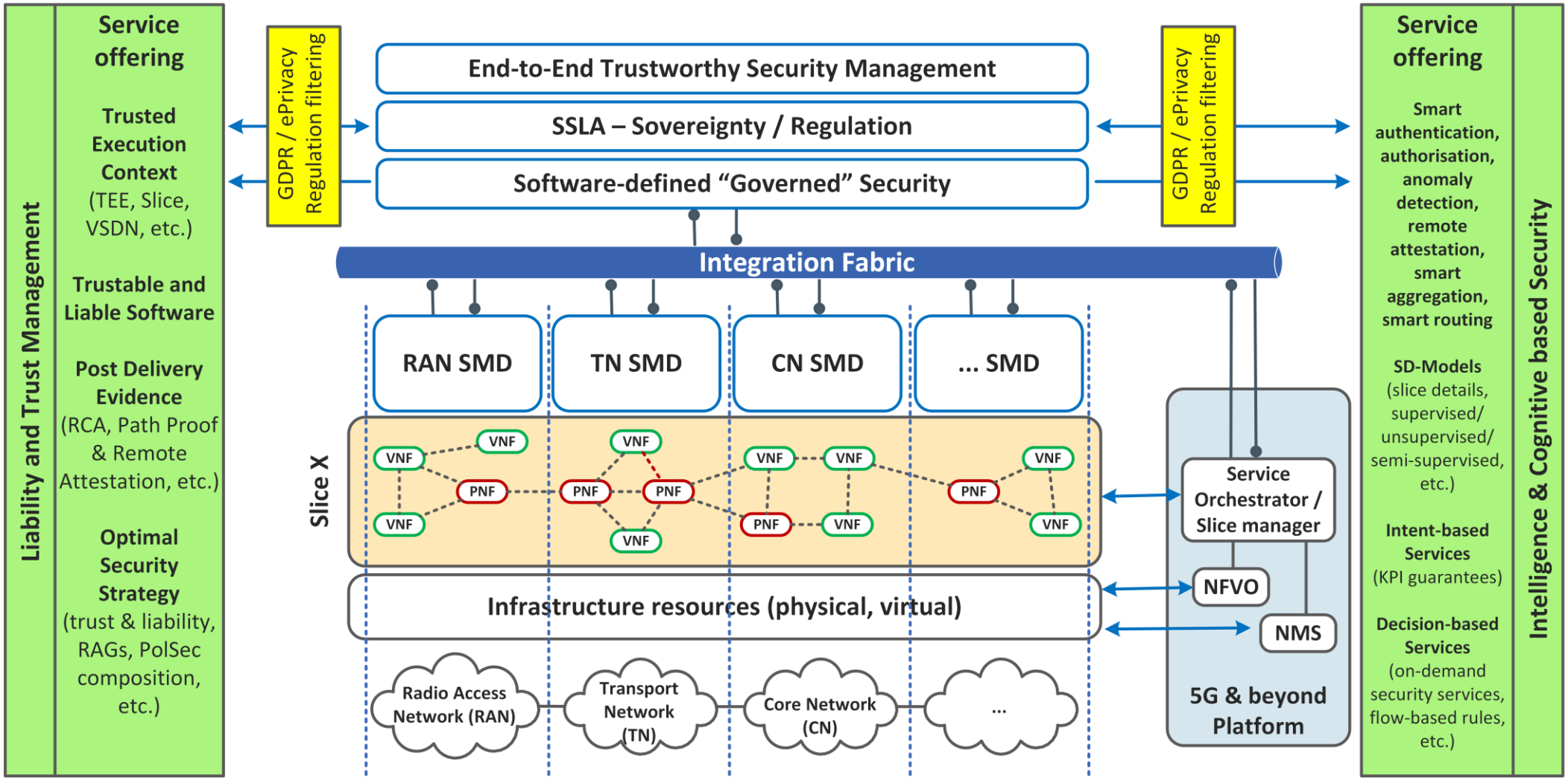
- Stakeholders' security requirements of 5G
  - Questionnaire for identifying business 5G security requirements
    - https://docs.google.com/forms/d/e/1FAIpQLSflwQjwIPsXGDG--RfGG8OM8wwqGY8aZAsjTmhbOpWz6d3MbQ/formResponse
  - 12 questions divided into three categories
    - Business and organisational requirements
      - What are the major threats you would like 5G services and applications to be protected from?
      - What critical features in terms of security of 5G infrastructure would you require to be improved?
      - What key security design improvements would you consider as a plus compared to your business activities? How would you like your personnel to be assisted in this regard?
      - What would be the business impact of a security incident for your organization?
      - What type of technologies of INSPIRE-5Gplus you consider are more likely to improve your security? Explain briefly why?
      - What key processes, policies, best practices on privacy and security in your organisation do you consider key for the use of the proposed INSPIRE-5Gplus?
    - Regulatory compliance and reputation requirements
      - What are the key standards and regulations your infrastructure has to comply with for security and privacy? How do you see INSPIRE-5Gplus can help to achieve this compliance?
      - What feature would increase your trust in relation to exchanging anonymous information about incidents within a closed group of 5G operators and providers?
      - Please describe possible usability requirements regarding the utilisation and deployment of INSPIRE-5Gplus which will be developed during the project (e.g., the tutorial of each components/processes should be available in different languages).
      - What availability tests do you consider necessary for testing the availability/efficiency of INSPIRE-5Gplus technologies you are waiting? Could you please specify what type of security KPIs are you expecting?
      - What are your availability concerns or issues? How do you think INSPIRE-5Gplus technology may assist you?
      - What kind of other improvements and/or technologies would like INSPIRE-5Gplus to implement and what are the expected value you would hope to derive from them?
    - Background information
      - What is your level of responsibility at your company?
      - What is industrial domain is your company involved?
      - What is your main job function?
      - In which world region(s) does your company offer services/products?

5G (& Beyond) Security Threats & Requirements

INSPIRE-5Gplus

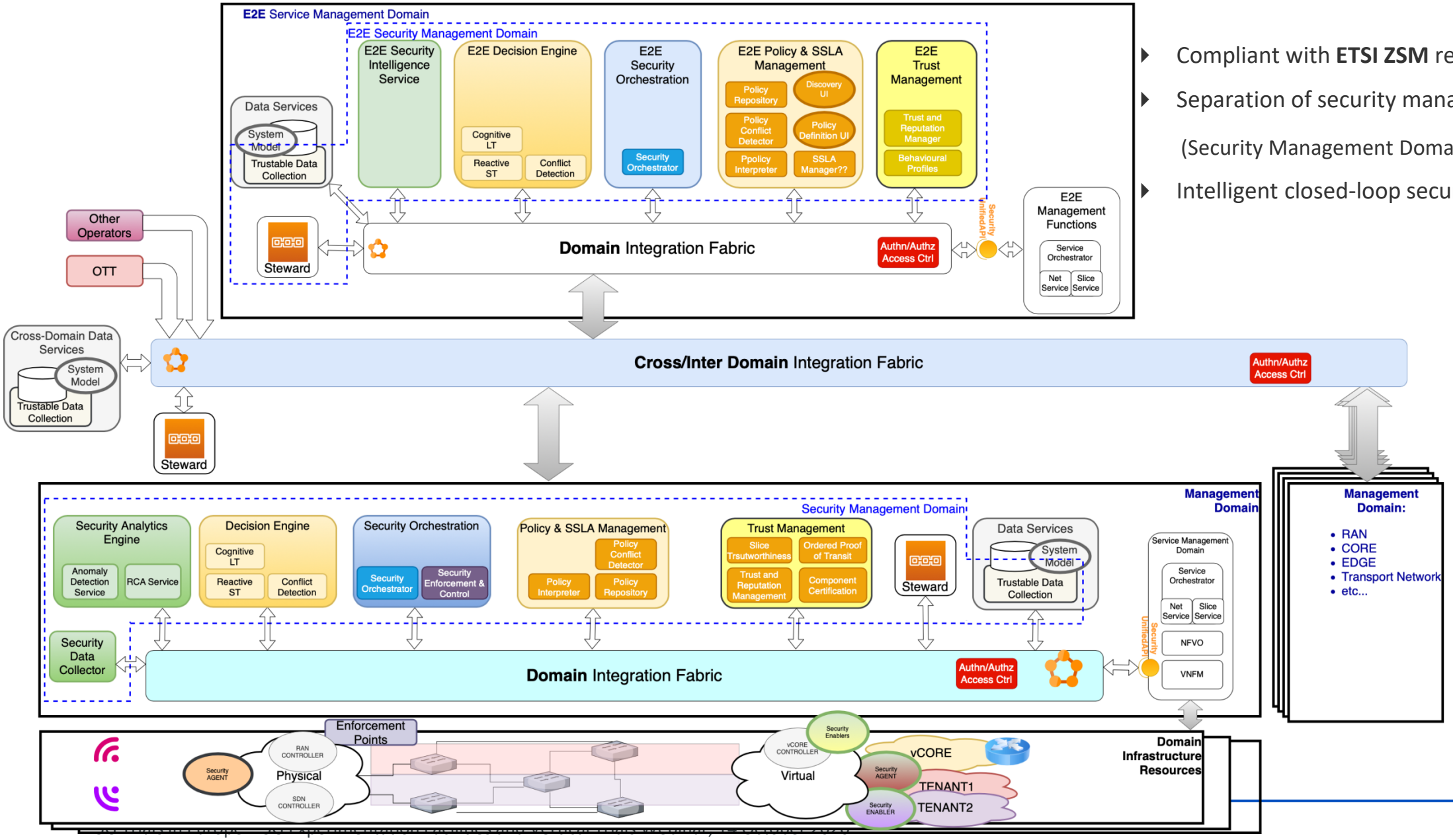
- Stakeholders' security requirements of 5G
  - The survey received **23 responses**
  - Several patterns were identified
    - **Major threats to protect against:** threats derived from virtualized assets (9 responses)
    - **Critical security features to improve:** monitoring (5), and sandboxing (4)
    - **Business impact:** loss of reputation (17), loss of revenue (8)
    - **Expectations on which technologies INSPIRE-5Gplus works at can improve security:** blockchain and trust (3), security analysis (3), monitoring (2)
    - **Key security processes:** security by design (4)
    - **Key standards and regularity requirements:** 3GPP (7), ISO 27001 (4)
    - **Usability requirements:** Online documentation and tutorials (15)

INSPIRE-5Gplus High-level Conceptual Architecture



INSPIRE-5Gplus Security Framework HLA

INSPIRE-5Gplus



- Compliant with **ETSI ZSM** reference architecture
- Separation of security management concerns

  (Security Management Domains (SMDs) + E2E SMD)
- Intelligent closed-loop security management

5G & Beyond Security Use Cases

INSPIRE-5Gplus

- 21 UCs (still evolving)
- Mapping of UCs to 5G-PPP projects
  - **3** projects ICT-17 – 5Genesis, 5G-VINNI and 5G EVE
  - **2** projects ICT-18 – 5G-MOBIX and 5G-CroCo
  - **2** projects ICT-19 – 5G!Drones and 5Growth

5Genesis

5G-VINNI

5G EVE

5G MOBIX

5GCroCo

5G!DRONES

5GROWTH

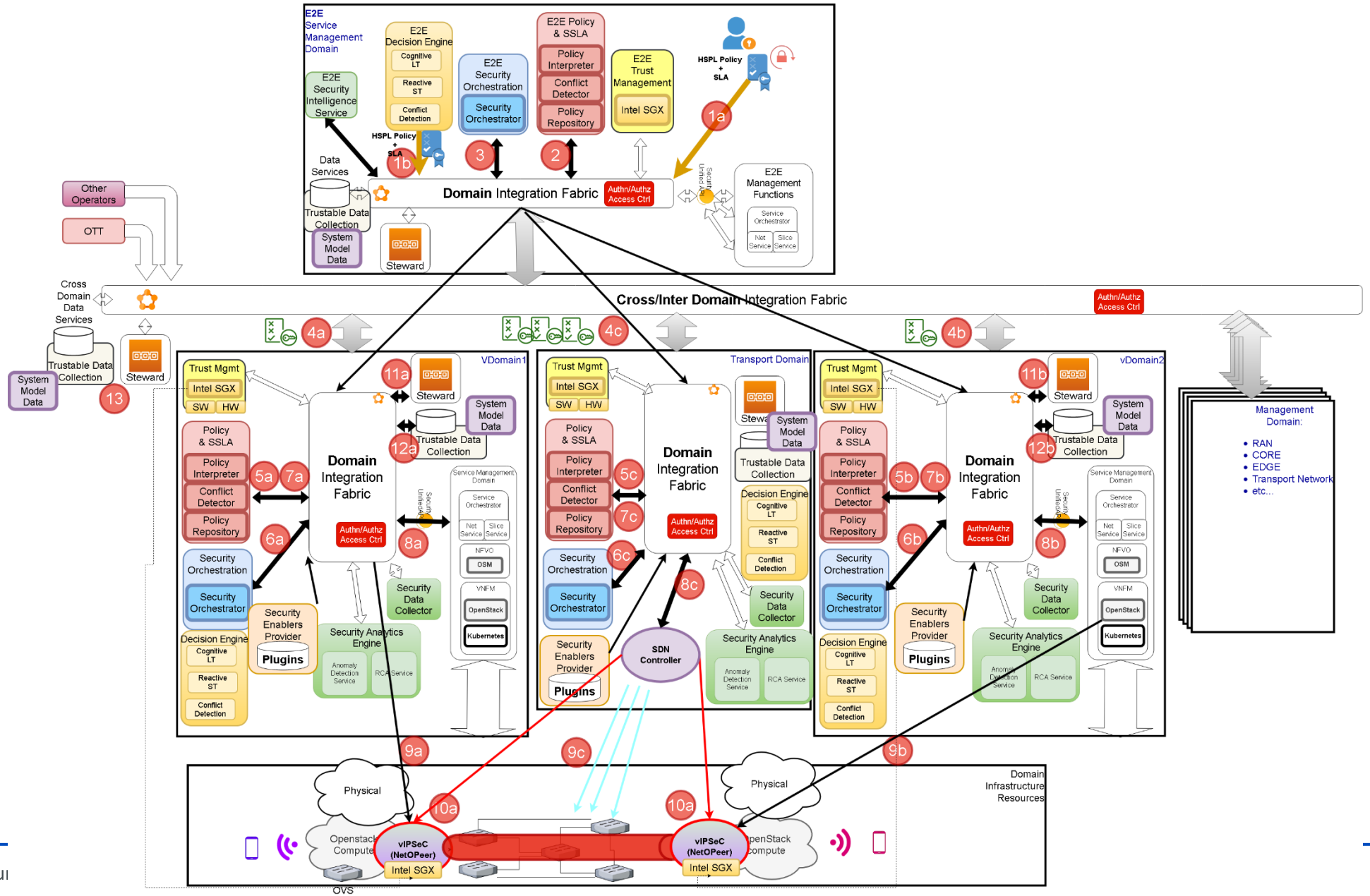
Illustrative UC - E2E Encryption TEE secured SECaaS

INSPIRE-5Gplus

- VNFs acting as proxies can be deployed dynamically to protect communications end to end.
  - IPSec and/or DTLS
  - The basis of both encryption systems is based on key derivation --> **centralized or on the hosts**.
  - Centralized:
    - IETF I2NSF (based on IKE)
    - Thales proposes SD-SEC
    - both having important similarities.
- While end-to-end communication may be encrypted
  - computer processor vulnerabilities lead to memory introspection (AES).
  - Take profit of SGX enclaves to perform encryption-decryption operations transfering native code to the TEE
  - protecting the delegated VNF security from other MEC node neighboring VMs.
- The **Objective** is to produce a Zero Touch solution based on Policy and sSLA definition that can be triggered automatically based on system state and data collection inputs.

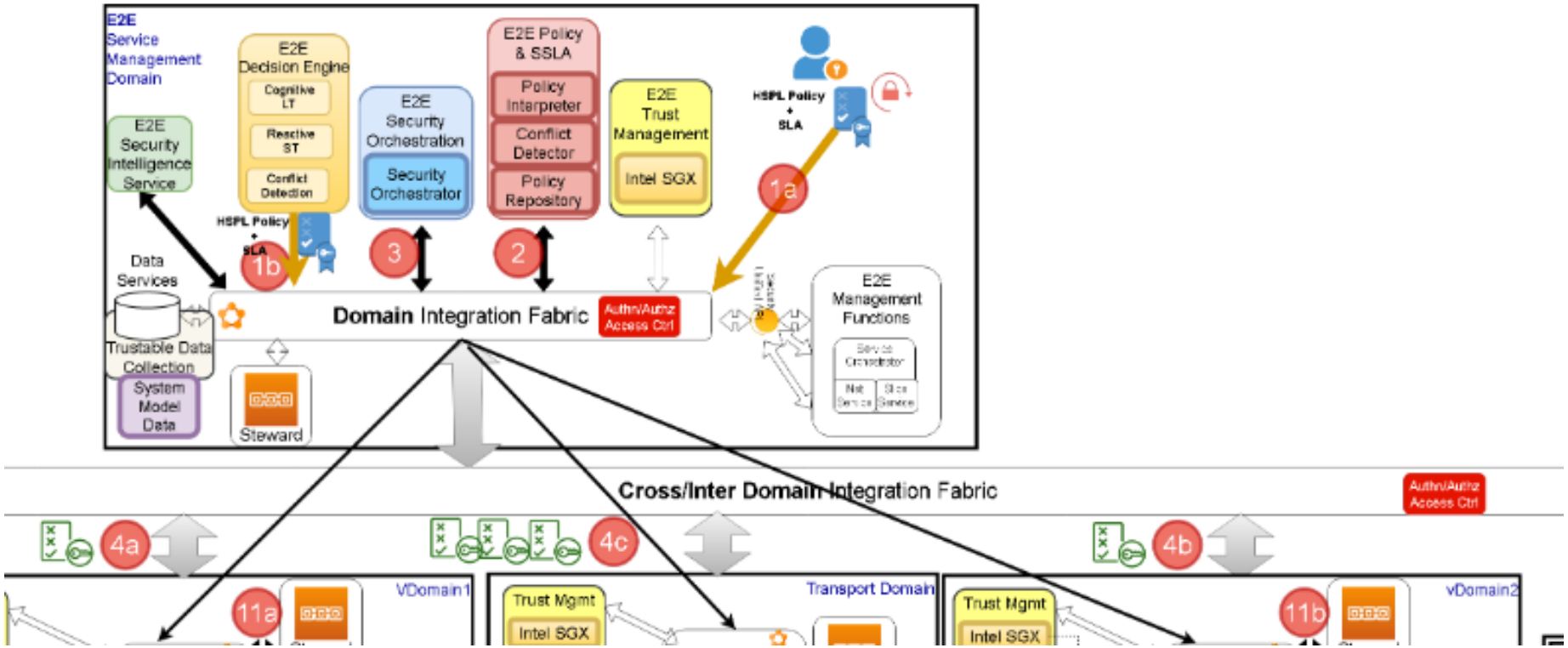
Illustrative UC - E2E Encryption TEE secured SECaaS

INSPIRE-5Gplus



Illustrative UC - E2E Encryption TEE secured SECaaS

INSPIRE-5Gplus

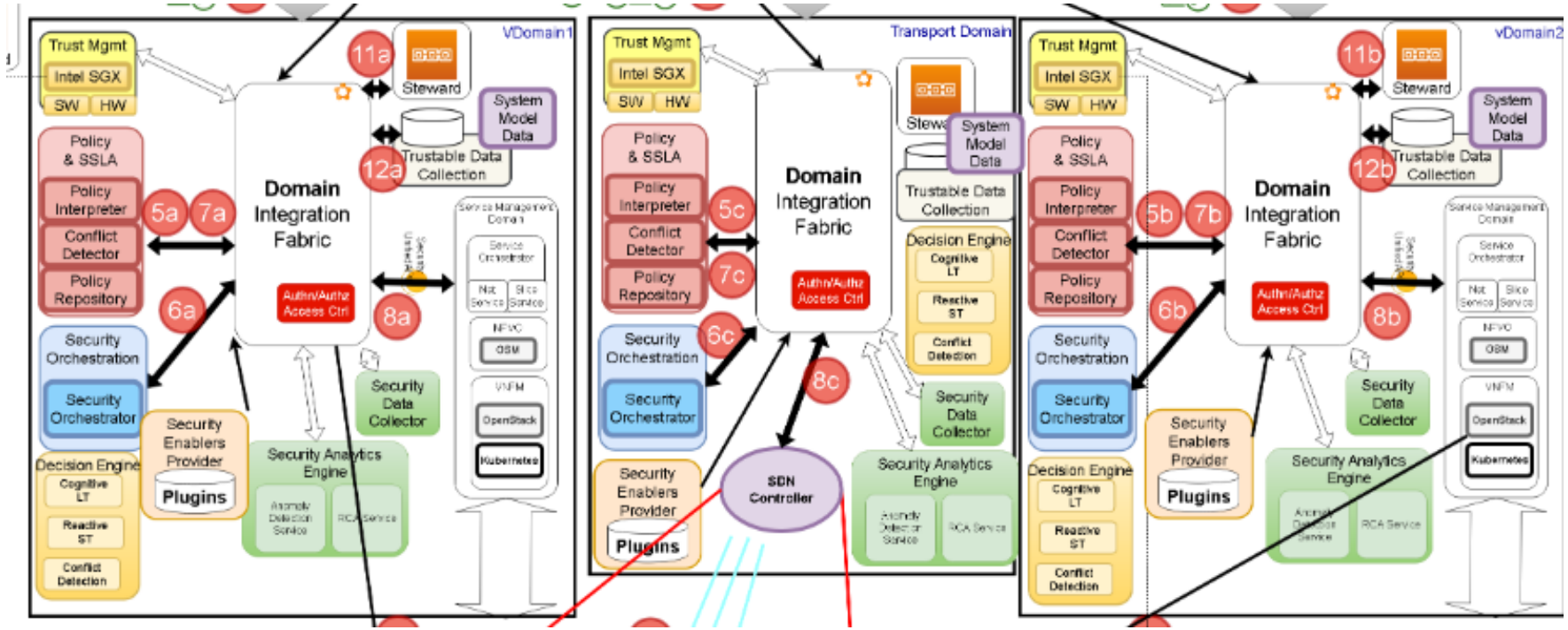


E2E SECaaS bootstrapping

1. HSPL4Orchestration + sSLA from Admin Security or E2E Decision Engine
2. MultiDomain Orchestration process starts by producing multi-domain policy refinement
3. Refinement is enforced (3 IPSec MSPL policies + 2 Forwarding traffic MSPL Policies)
4. Each Domain receives a MSPL policy that can be addressed by each Domain independently

Illustrative UC - E2E Encryption TEE secured SECaaS

INSPIRE-5Gplus



Parallel domain enforcement

5-8 Each domain produces a refinement from the received MSPL into a specific action on the infrastructure.

- vDomain1 and vDomain2 trigger IPSeC VMs through MANO. Also configure TEE
- Transport Domain triggers SliceManager to provide connectivity between VMs and deploys keying material

11-12 operational and statistical data is stored for further usage. E.g., in Cognitive Long-Term Decision Engine

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 Nº 871808. The European Commission has no responsibility for the content of this presentation.