Towards 5G Embedded Trust

Integrating Attestation Extensions in Vertical Industries

Thanassis Giannetsos, **Dimitris Papamartzivanos**, Sofia Anna Menesidou, Sophia Karagiorgou
Digital Security and Trusted Computing Group
Ubitech Ltd.

EuCNC FAST Workshop 2021

Key Messages as we are Moving Forward

- **Distributed:** All CPSoS must be seen as inherently and increasingly Federated Safety Critical Systems which are not owned by a single entity
  - “Systems-of-Systems” – *Multiple components from different OEMs which you don’t trust*

- **Security, Privacy, Trust interchangeable models over the infrastructure/edge continuum**
  - Overcome challenges and limitations of existing PKI-based architectures
  - Scalability, Performance, Privacy, Trust – *Strong security assumptions*

- **Bottom up: Particularly with respect to Safety, data and system components must be in position to make strong statements about their (run-time) integrity**
  - *Need to make sound statements on software security properties of single systems and transfer these on the security properties of hierarchical compositions*

- **Defensive:** Static defence techniques will not be enough in the face of a wide range of attacks

Software eats the world….and what's left is data

"103 exabytes of data is generated by vehicles every day" – IBM

- ✓ Telemetry data which can be used for maintenance
- ✓ Data transmitted by connected components need to be authenticated
- ✓ Data protection is essential

- ✓ Safeguards code updates against tampering
- ✓ Ensure that firmware and software code comply with internal policies
- ✓ Over-the-air reprogramming

- ➢ **No security mechanisms on isolation** - *obsolete*
- ➢ **Devices as standalone components or single entities** – *part of a Service Graph Chain*
- ➢ **Establish and manage trust between "entities" and the "network" and vice versa**

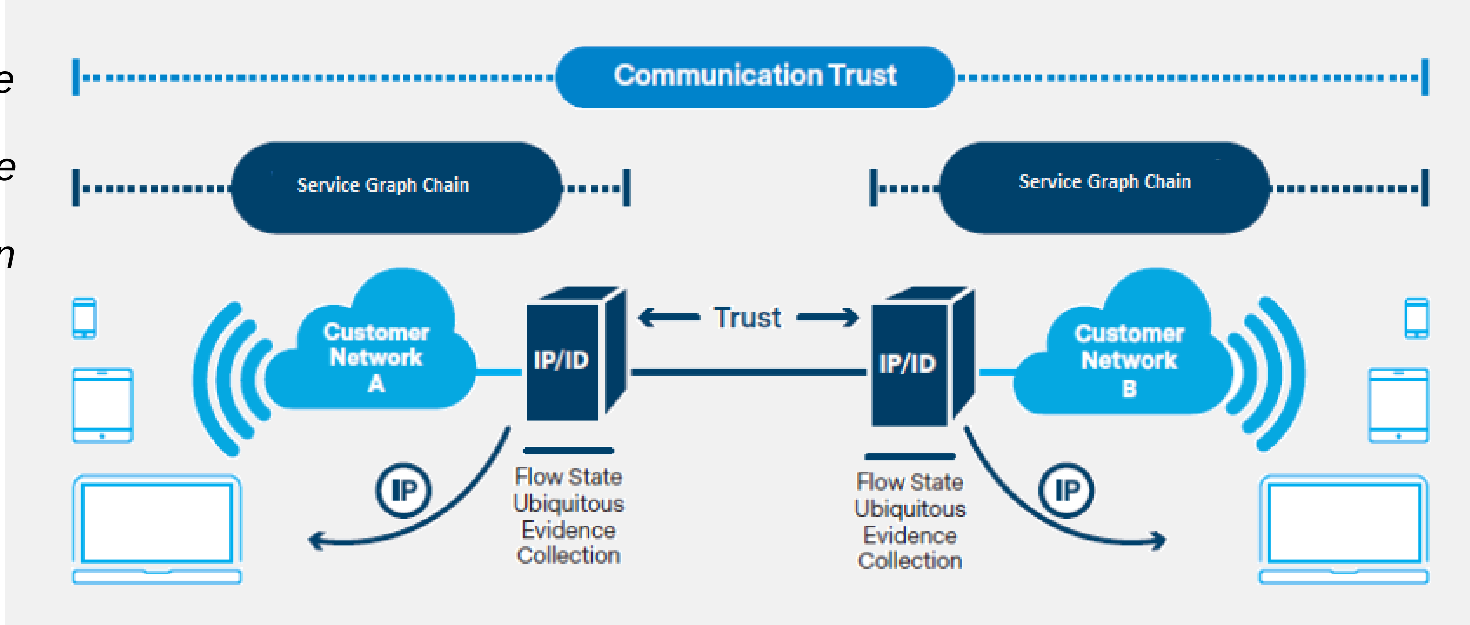
Towards Trust Aware Service Graph Chains (SGCs)

Remember till now security and safety were two distinct goals BUT…

- **Industry is now interested in converging security and safety**
  - Contradicting requirements – *Security might impede safety*
  - *Strict requirements in terms of latency, reliability and seamless service delivery*

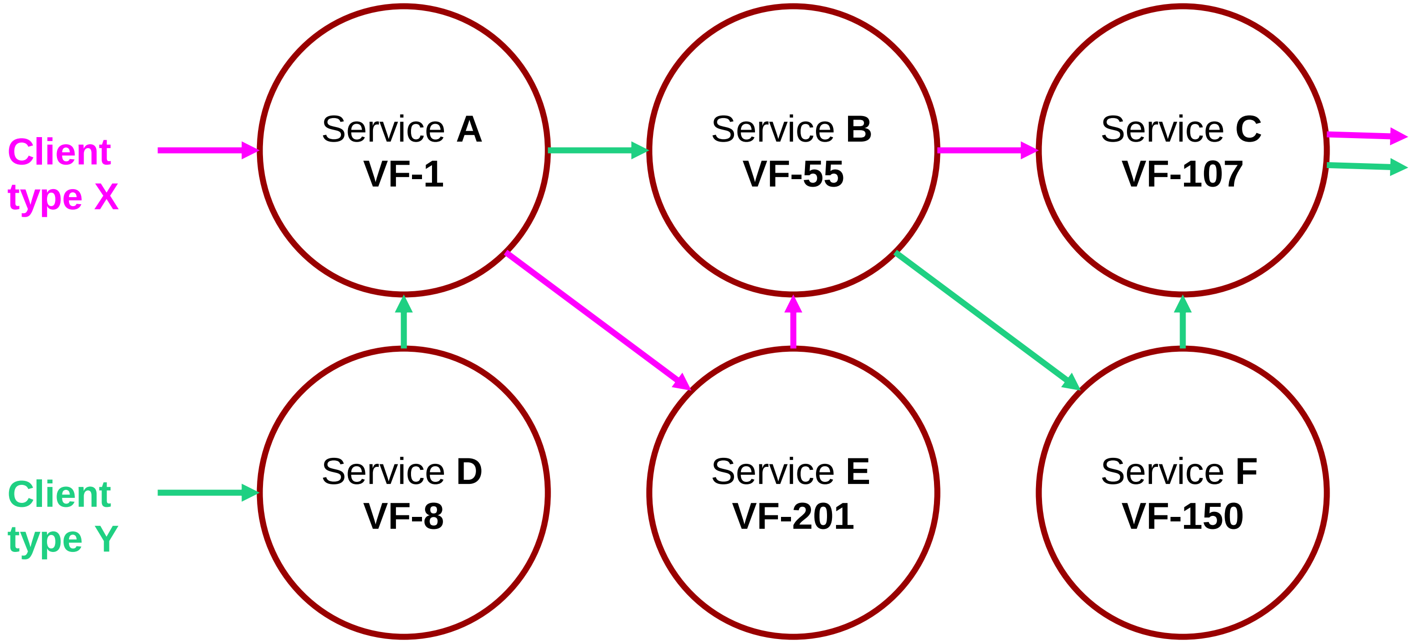
- **Fundamental issue of trust or trustworthiness –** *Remote platform behaves in a reliable and predictable manner*
  - **Trust to the EDGE** – *Do I trust the EDGE device to calculate on my behalf?*
  - **Trust the NETWORK** – *Do I trust the input given by other platforms? Compromise or malfunction*

- **Trust Aware SGCs:** Platforms and their running services must be enabled to make and prove statements about their state and actions so that other component of a SGC can align their actions appropriately and an overall system state can be evaluated and enforced



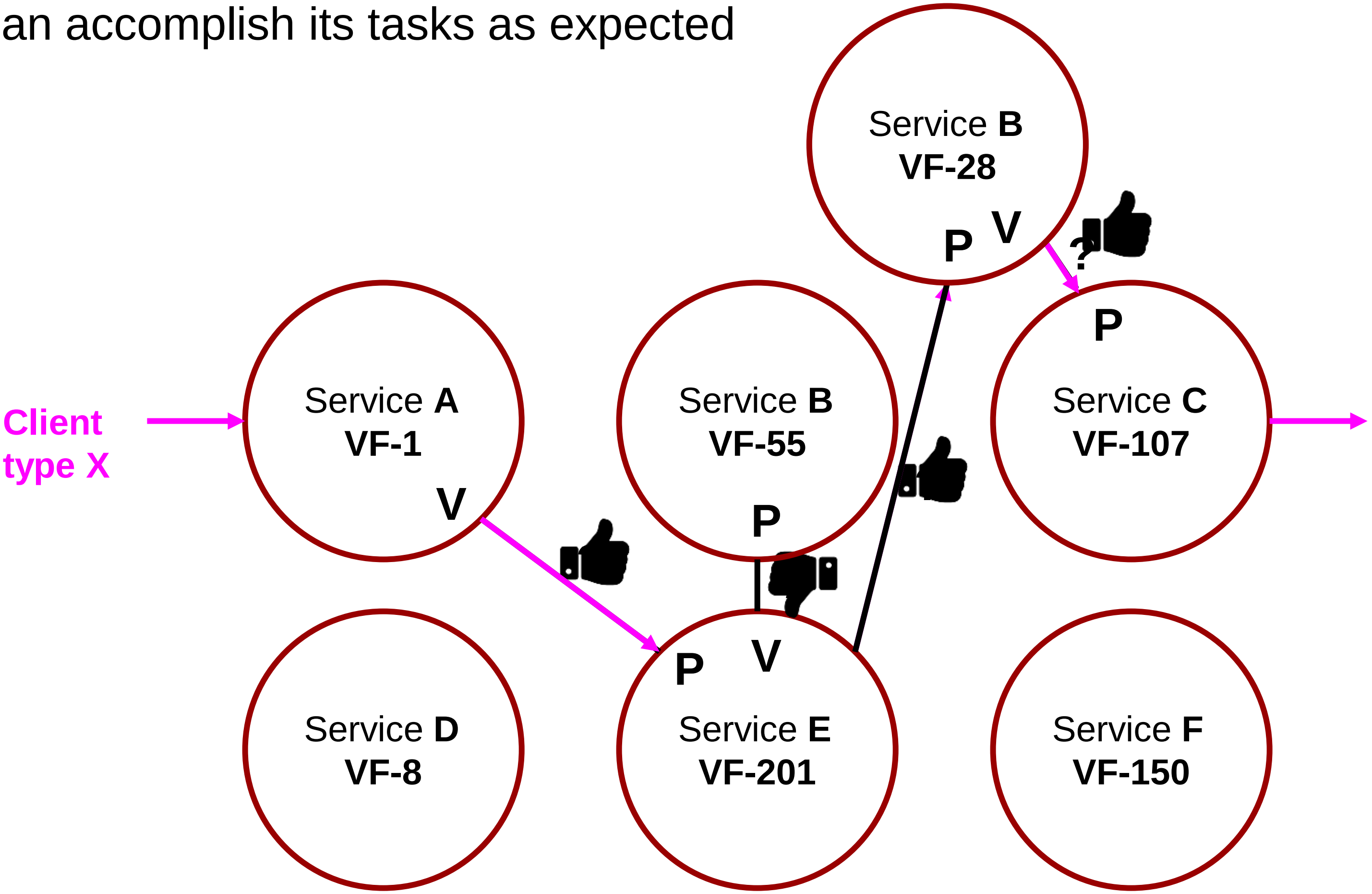
What we want and why

- Infrastructure services transition from physical to software (virtual) functions (VFs)
  - VF chaining enables the creation of composite (network) services that consist of an ordered set of VFs
- Each VF in a path (i.e., Service Graph Chain, SGC) should be able to **securely**, **effectively** ascertain the correctness of the **configurations** of its adjacent VF (next hop)



Remote Attestation (RA)

- Enables a system (the verifier, **V**) to determine whether another system (the prover, **P**) can accomplish its tasks as expected



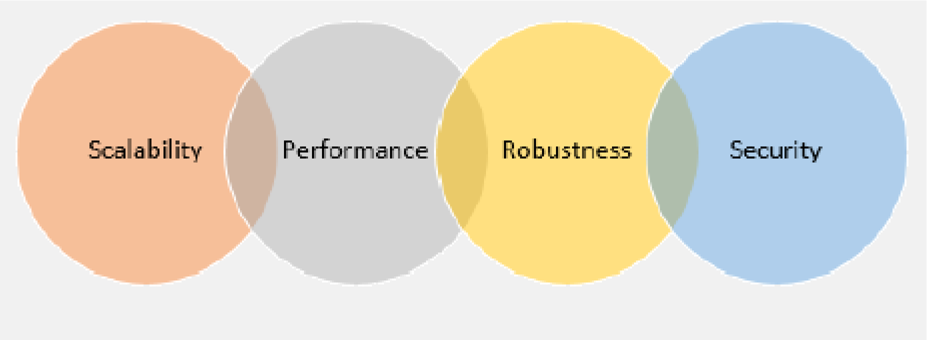
Other RA Schemes

Property-Based Attestation (PBA)

- Mapping the platform configurations to attestable properties
- Improves the complexity of the **Verifier** who simply has to determine whether the **Prover** satisfies certain properties
- **The problem is identifying sound and generic properties when considering SGCs comprising mixed-service and real-time VFs**

Hybrid Solution:

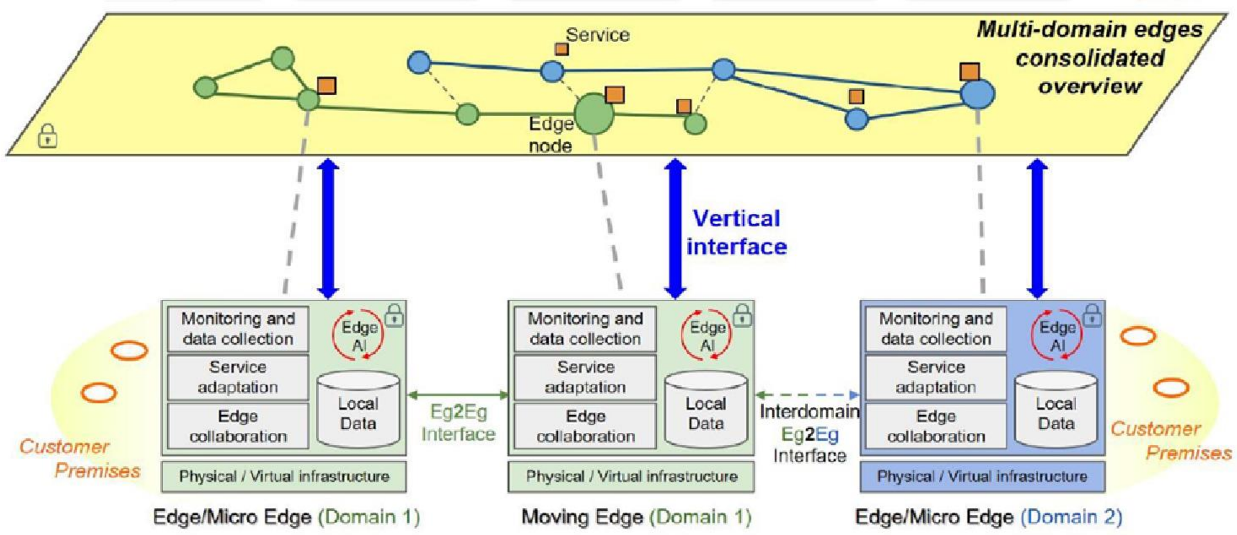
- Provide the necessary means to ensure the privacy-preserving property of PBA while retaining the profoundness of BBA



So is that all….

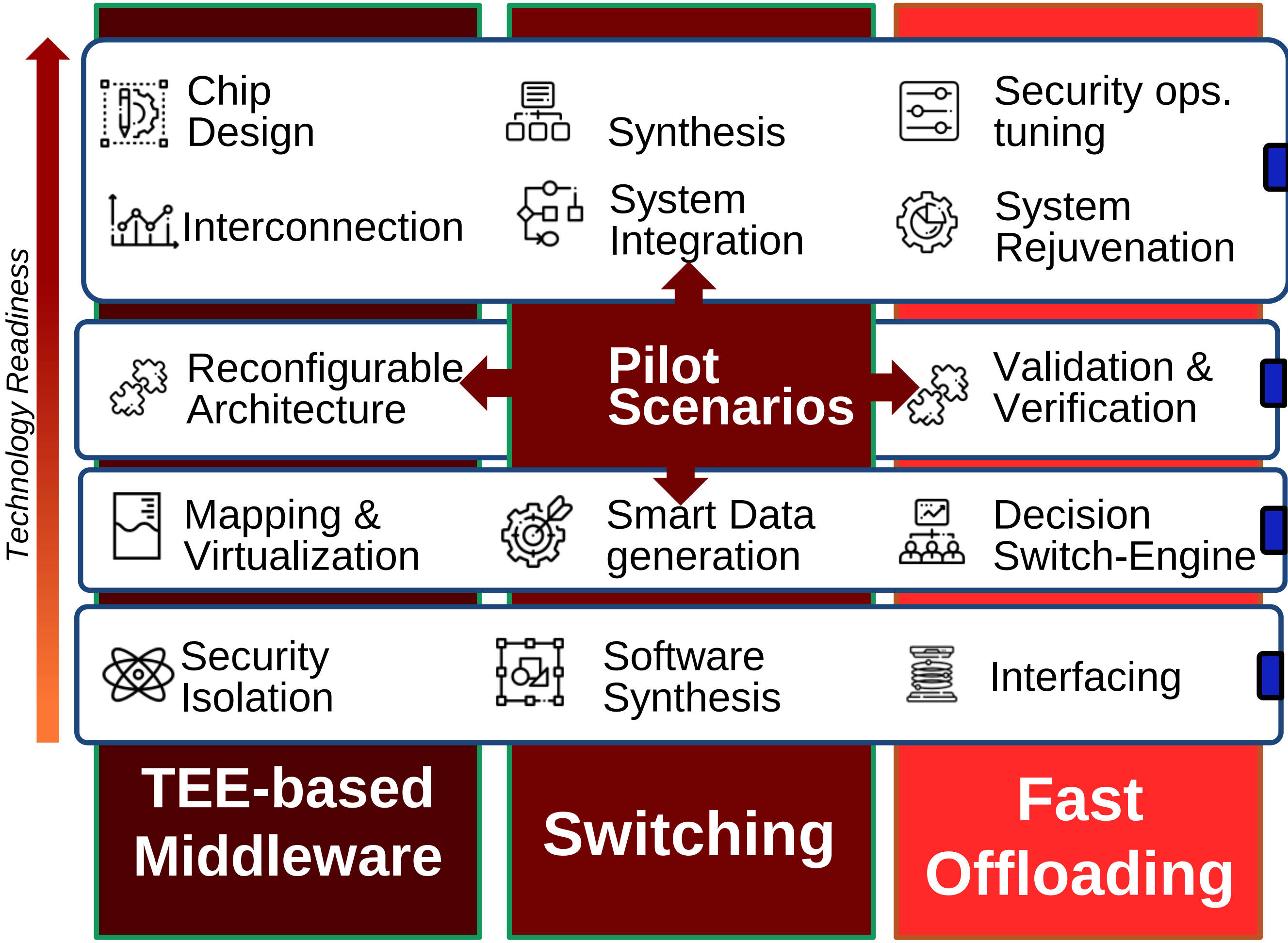
- **5G is the vehicle towards realizing next-generation smart-connectivity "Systems-of-Systems" (SoS)**
  - Managing service graph chains for highly distributed and heterogenous services (cyber-physical end devices, to edge servers and cloud facilities and microservices)
  - Provision of **mixed-criticality services** in several vertical industries
    - Strict performance and security requirements

- **Goal**:
  - Enable high scalability by **decomposing a mixed-criticality application** into a set of **"cloud-native"** and **"edge-running"** microservices, with different trust considerations, and managing secure accelerated offloading capabilities for distributing the resource intensive processes to the backend, thus, limiting the workload that needs to be managed at the edge.

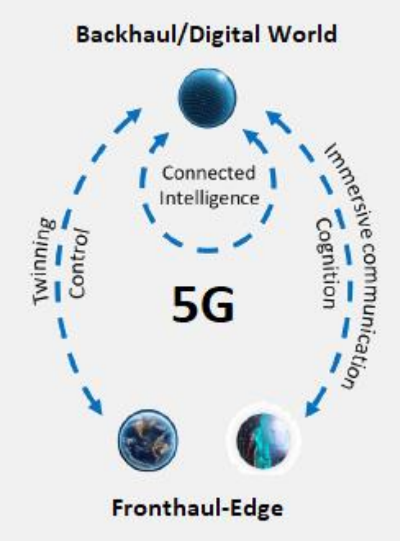

Multi-domain edges consolidated overview
Service
Edge node
Vertical interface
Monitoring and data collection
Edge AI
Service adaptation
Local Data
Edge collaboration
Physical / Virtual infrastructure
Eg2Eg Interface
Interdomain Eg2Eg Interface
Customer Premises
Customer Premises
Edge/Micro Edge (Domain 1)
Moving Edge (Domain 1)
Edge/Micro Edge (Domain 2)

Mixed-Criticality Services

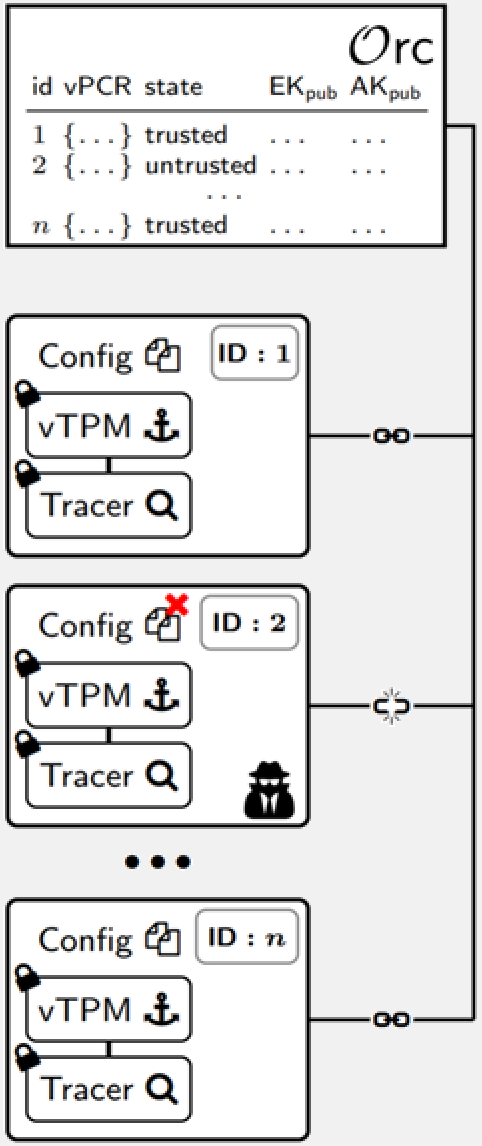
- **NFV & MEC intelligent orchestration to orchestrate and optimize the whole process**
  - “application orchestrator” needs to be responsible for managing the lifecycle of all deployed microservices
  - offloading the resource intensive non-safety-critical operations from the edge to the backend infrastructure
  - Leave “room” for the execution real-time, “edge-running” and latency free safety-critical services that need to operate in strict security boundaries
- **Secure Edge Processing**



Envisioned Architecture

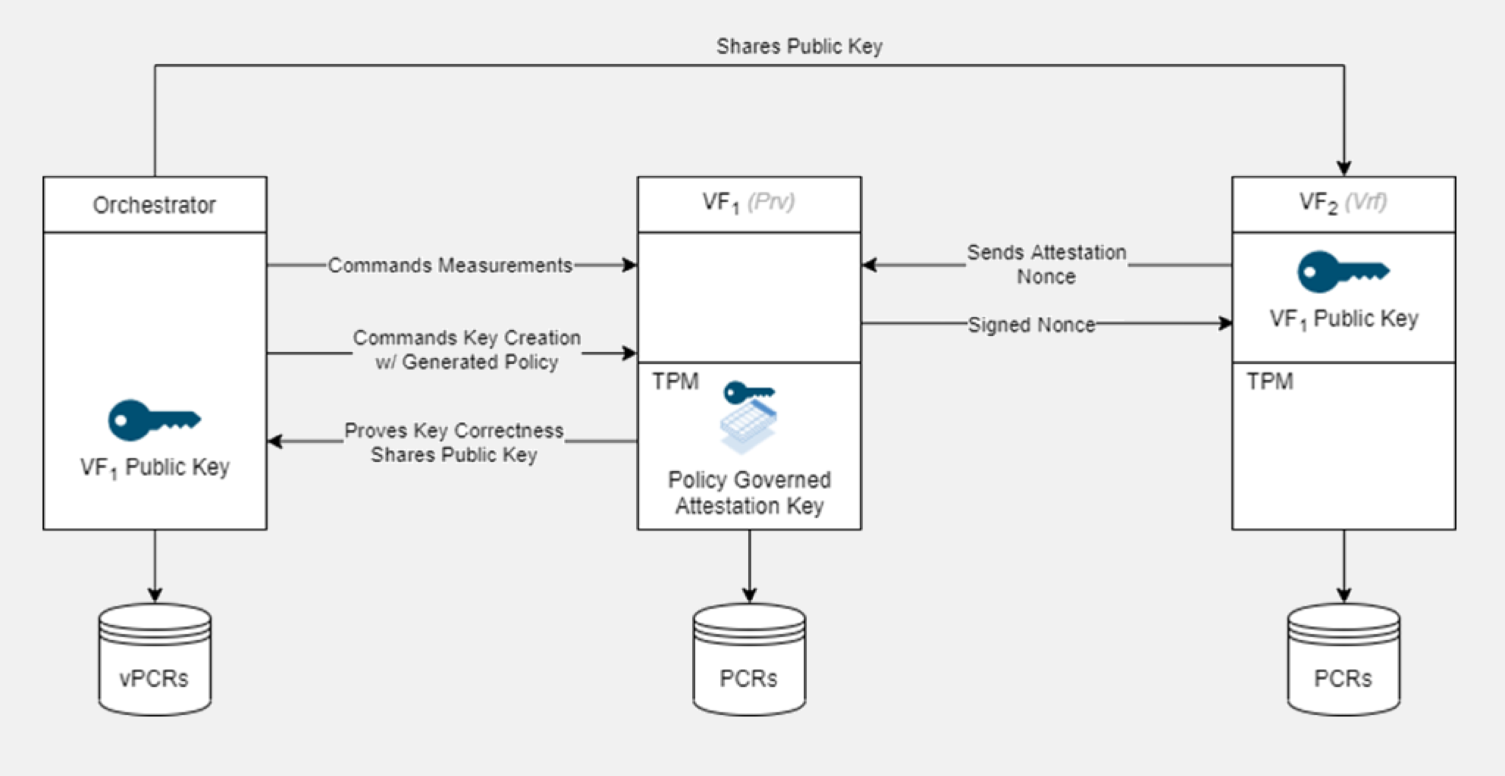


- Orchestrator deploys VFs and manages configuration updates
  - Trusted state is reflected in vPCR associated with the VFs
- ***Digital Twin as an extension of the physical world to the digital world***
- Desirable system properties:
  a. **P-1:** VF Configuration Correctness: ensure load- and run-time configuration correctness
  b. **P-2:** SGC Trustworthiness: ensure **P-1** throughout all SGCs
  c. **P-3:** Attestation Key Protection: the AK is created securely
  d. **P-4:** Immutability (Tracer): the execution of the Tracer is immutable



id	vPCR	state	EK_{pub}	AK_{pub}
1	{...}	trusted	...	...
2	{...}	untrusted	...	...
		...		
n	{...}	trusted	...	...

Privacy Preserving VF2VF Attestation

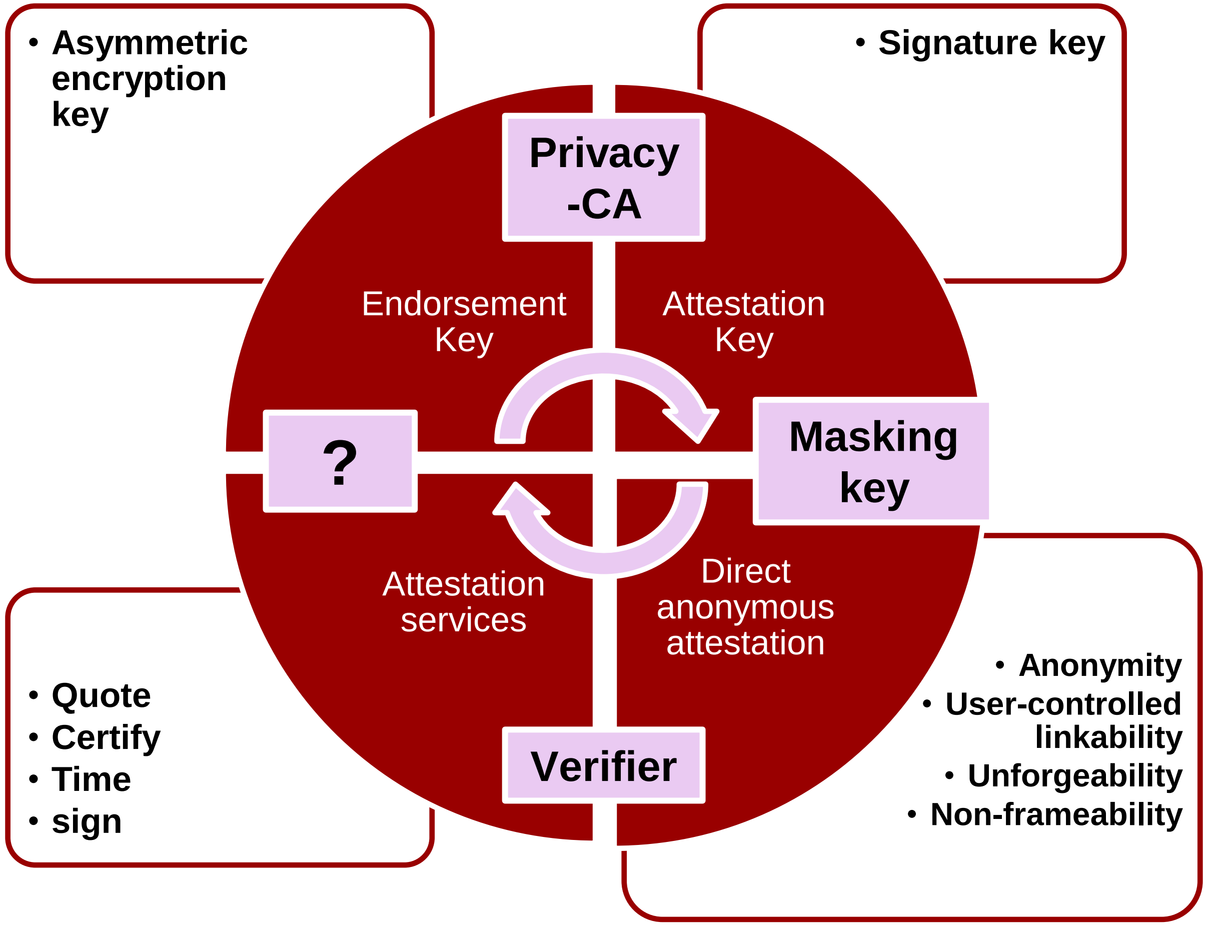


We need to build a root of trust

- Because today’s computing systems are too complex to be trusted in one go, we have to start from somewhere
  - **No one size fits all solution** – select and tailor approach to requirements

- To build a trusted computing system, one needs first to choose a root of trust
  - Hardware vs. Software ROT – TPMs vs. TEEs
  - Work together?
  - *A TEE can be seen as a secondary ROT which is initialized by the primary TC*

- There are many challenges in building such a root of trust
  - *Cost, Assurance, Tamper Resistance, Functionality, etc.*



Example Industries

From Fog/Edge/Cloud Computing

- Deployment, Orchestration and Data Management for scalable and secure fog/edge/applications (**RAINBOW**)
- Decouple security orchestration from application business logic (**ASTRID**)
- Security of all actors/entities in supply chains (**ASSURED**)
- https://rainbow-h2020.eu/, https://www.astrid-project.eu/
- https://www.project-assured.eu/

To Secure Societies/SMEs

- Cyber security "As-a-Service" for business ecosystems
- Dynamic monitoring and forecasting of threats
- **Optimal security policies recommendation for SMEs&MEs**
- Threat intelligence data marketplace through the integration of Blockchain
- https://puzzle-h2020.com/

RAINBOW

ASTRID

ASSURED

PUZZLE EU Project

Wrapping it Up

Benefits of Trust Aware Service Graph Chains (SGCs)

- One of the main challenges is the lack of sufficient trust when it comes to the behavior of a remote system that generates and process mission critical and/or sensitive data.
- Guarantee the **correctness and integrity of the generated data flows**
- **Personalized cybersecurity functions** in multi-tenant environments
- **Definition of trust zones** - distinct pockets of infrastructure with same trust and safety-critical mission
- Minimizing malicious threats to affect safety-critical applications

Questions?