CASTOR Project Launches to Pave the Way for Trusted Communication in the Compute Continuum

ATHENS, 21st of October 2024 - ***The project CASTOR, an ambitious initiative aimed at addressing the growing challenges of secure and trustworthy communications within the compute continuum, has officially been launched.***

The shift from cloud-centric services continues to accelerate (due to their limitations in meeting emerging end-user needs) and compute functionality is increasingly moving closer to the edge. This change has given rise to the concept of a "compute continuum", where resources and computing capabilities are dispersed across cloud, edge, and user equipment. The new architecture poses challenges in ensuring end-to-end security, as the workloads traverse untrusted and continuously changing hardware and software infrastructures.

The project CASTOR, funded under the *Horizon Europe Innovation Action* program, aims to develop and evaluate cutting-edge technologies to enable trustworthy, seamless, and efficient communications across distributed infrastructures at the edge and far-edge of networks.

At the core of CASTOR's innovation is the development of a system that will process and convert the high-level user requirements into a combination of security needs and network resource "policies". These policies are then enforced on continuum hardware and software, resulting in an optimized, trusted communication path that can adapt to changing trust states in the continuum.

Key Innovations of CASTOR Include:

- **Composable and Distributed Attestation**: CASTOR enables distributed attestation across compute nodes in the continuum, with adaptive mechanisms to quantify trust in real time.
- **Optimized Trust-Based Path Derivation**: The project introduces methods to derive the most secure and efficient communication path by jointly considering the trust properties of the continuum infrastructure and the available resources.
- **Vendor-Agnostic Trusted Communication**: CASTOR ensures trusted communication across heterogeneous infrastructure, crossing multiple administrative domains without being limited by vendor-specific solutions.

The CASTOR Consortium, a collaboration of leading university researchers and industry experts from the fields of telecommunications, aerospace, cybersecurity, and data intelligence, recently held a productive meeting to align on the key project developments.

With this occasion, Daphne Galani, the Project Coordinator of CASTOR, declared: *"CASTOR represents a significant step forward in enabling secure and trusted communications across the compute continuum. As computing shifts to the edge, we must ensure that the infrastructure supporting these critical workloads is resilient, adaptable, and secure. Our Consortium team is focused on developing innovative solutions that will create optimized, trusted communication paths across a wide array of infrastructures. We believe the outcomes of CASTOR will not only address the existing gaps, but also help shape future standards in trusted communications."*

The project CASTOR will be tested in real-world use cases, involving the sharing of security and safety-critical information within Connected Cars and Automated Mobility, drones which form Flying Ad-Hoc Networks and Airspace industry applications. CASTOR's technologies will be validated through carefully designed testbeds. The findings will contribute to the growing body of knowledge on trusted communications and will feed into the development of trust-relevant standards currently being addressed by the Internet Engineering Task Force (IETF).

If you are interested in tracking the development of the project CASTOR, follow the it on **X/Twitter** and **LinkedIn** channels. Further information will be provided soon on **https://castorhorizon.eu/**.

About project CASTOR:

The project CASTOR (*Continuum of Trust: Increased Path Agility and Trustworthy Device and Service Provisioning*) is a cutting-edge research project focused on advancing trustworthy communication across the compute continuum. It is powered by a Consortium of 16 members which have complementary expertise in aerospace, cybersecurity, communications, data intelligence, IoT and telecommunication: UBITECH(Greece), QUBITECH (Greece), Mellanox Technologies LTD(Israel), University of Surrey (UK), Orange Romania (Romania), Technical University of Iasi (Romania), Collins Aerospace Ireland (Ireland), ICCS (Greece), University of Kent (UK), Suite5 (Cyprus), K3Y (Bulgaria), Wings (Greece), University of Murcia (Spain), Feron Technologies (Greece), COMMSIGNIA(Hungary), University of Amsterdam (Nederland), Digital for Planet (Switzerland).

Media Contact: olivia.ciubotariu@digital4planet.org