

About CASTOR

Funded under the Horizon Europe Innovation Action program, the project CASTOR is a multi-disciplinary research initiative that focuses on **ensuring the trust-aware establishment of network routing paths** as part of the traffic engineering process.

Overall, CASTOR's vision lies in the construction of **a trust plane capable of engraining trust throughout the entire Computer Continuum (CC)**.

By embedding novel trusted extensions in each routing element that can expose trustworthiness evidence in a verifiable manner, **CASTOR enriches existing orchestration mechanisms** with capabilities for establishing secure, trusted, and optimized service-graph-chains across the entire Compute Continuum, under the principle: "Never Trust, Always Verify."

By advancing the state-of-the-art in networking and (sub-) zero-trust domains, CASTOR brings key innovations in the standard-track Path Computation Element (PCE) extensions across different CC layers and operations. It designs a generic methodology enabling the dynamic, continuous (evidence-based) trust assessment of complex topologies and enforcement of dynamic (segment-routing) policies. Allowing the elevation of node-centric trust evaluations to trust characterizations over the entire topology, **CASTOR enables trust- and network-aware traffic engineering decisions**.

Today's routing technologies rely on somewhat obsolete decisions based on the availability of network and computing resources. As an alternative, **CASTOR combines novel adaptive-to-change mechanisms** for capturing a device's (HW and SW) trust scores, anchored to a custom Trusted Computing Base (TCB), **enabling CC-wide trust quantification and inter- and intra-domain trusted path establishment**.

CASTOR Technology Stack

- 1. Trust- and Network-Aware Path Establishment:** Enabling cross-domain path routing to meet strict trust and resource needs for mixed-criticality services.
- 2. Adaptive Trust Quantification:** Establishment and maintenance of an up-to-date view of the trust state of each CC device, enabling the routing of network workloads over the path that can exhibit the Required Trust Level.
- 3. "Chip-to-Cloud" Security Assurances:** CASTOR manifests novel (composable) attestation schemes for the verifiable (and privacy-preserving) monitoring of device- state evidence based on which their trust characterization can be conducted.
- 4. Combinatorial Trust and Resource Optimization:** CASTOR uses Quantum Annealing to solve the computationally hard (NP-hard) trusted path routing problem in hyper-dimensional networks, optimizing multiple path segments to meet diverse network and trust needs.

CASTOR applicability

CASTOR's technologies will be validated through four real-world use cases that involve sharing security and safety-critical information across various administrative domains and for different types of topologies exhibiting complex and diverse trust and network-resource usage requirements:



The consortium



Building Trust
in the Computing Continuum

More on castorhorizon.eu

Follow CASTOR

@castorhorizon-eu

@CASTORHorizon



www.castorhorizon.eu

Discover more
on CASTOR website!

