P2CODE

Programming Platform for
Intelligent Collaborative Deployments

Security & Trust

Trust built-in: secure, verified, and compliant by design

Visit our website and
follow us on Social Media

Funded by
the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Funded by the European Union (P2CODE, 101093069). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

P2CODE in Context

The P2CODE Architecture enables automated, trustworthy orchestration of services across federated, multi-domain environments—supporting critical use cases in Industry 4.0, mobility, healthcare, and beyond.

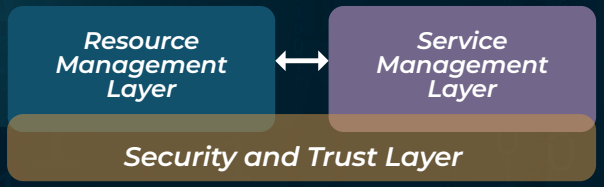
At its core, P2CODE is built on a layered architecture that is **modular, secure, and developer-centric.**

Within this design, the **Security & Trust Layer (ST-L)** ensures that all services and resources run in a trustworthy way—embedding security, compliance, and resilience into every part of the IoT–Edge–Cloud continuum.

What It Does

The ST-L secures identities, devices, software, and data flows across the continuum. It enforces zero-trust principles, verifies authenticity, and provides traceability to build trust in distributed, multi-domain environments.

P2CODE Open Platform



Core Components

1. **Maestro**
   The conductor orchestrating services across the continuum
2. **Secure Access Control**
   Role-based permissions with audit logging
3. **Policy & Telemetry Engine**
   Governs performance and rules in real time
4. **Internal Developer Platform**
   Unified dashboard from code to deployment

Key Benefits

- **Zero-Trust Service Access**
  Fine-grained identity & access control
- **Multi-Layer Attestation**
  Verifies hardware, devices & software integrity
- **Decentralized Identity**
  Verified IDs for people, services, and devices
- **Attack Mitigation**
  Real-time threat detection & response
- **Data Provenance**
  Tamper-proof audit trail of data origins & usage

Trust Flow Across Layers

- Validates service integrity (SM-L)
- Attests device trustworthiness (RM-L)
- Logs operations for compliance & auditing

Why It Matters

- Builds trust and resilience in distributed, multi-domain systems
- Protects critical services from cyber threats
- Ensures compliance with EU digital trust and sovereignty rules

Strategic Impact

1. **Developers**
   Security by default without added complexity
2. **Operators**
   Manage infrastructure safely and reliably
3. **Enterprises**
   Meet compliance and regulatory obligations
4. **Society**
   Protect sensitive services and data