**Uwe Roth**
Luxembourg Institute of Science and Technology
5, avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
uwe.roth@list.lu

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

# HORIZON-CL2-2026-01-DEMOCRACY-08
# ELECTORAL INTEGRITY IN THE DIGITAL CONTEXT
# EXPRESSION OF INTEREST

## Our Value Proposition

We provide the technical foundations of democratic trust.

While electoral integrity is a social and legal construct, it requires a secure, transparent, and auditable digital infrastructure.

The Cybersecurity group of the Luxembourg Institute of Science and Technology (LIST) specializes in bridging high-level democratic principles (such as anonymity, transparency, and auditability) with robust, field-ready cryptographic implementations.

Within a multidisciplinary consortium, LIST contributes and can lead applied cybersecurity activities translating democratic trust principles into secure electoral infrastructures, lifecycle threat modelling, and authenticity assurance mechanisms for electoral information ecosystems, while providing cross-cutting trust and security support across technical and governance components.

## Core Contributions and Pillars

In the context of this call, integrity extends beyond data protection to the holistic assurance that electoral processes remain free from manipulation across their full lifecycle.

LIST structures its contribution through three complementary Integrity Pillars supporting technical robustness, democratic legitimacy, citizen trust, and inclusive participation in digital electoral processes.

### Pillar A. Vote Integrity Layer: Verifiability

**The Problem:** Public scepticism toward opaque black box digital voting systems undermines trust in election outcomes.

**The Goal:** Restoring trust by enabling transparent and independently verifiable vote casting and counting processes without compromising ballot secrecy.

**The Contribution:** A framework for End-to-End (E2E) verifiability providing publicly auditable evidence that votes were cast and counted as intended. The framework enables electoral authorities, observers, and civil society to verify election integrity while preserving voter anonymity, including reference architectures, verification toolkits, and implementation guidelines.

**The Technology:** Leveraging advanced cryptographic verifiability mechanisms such as homomorphic encryption, zero-knowledge proofs, and related privacy-preserving assurance techniques to provide mathematically verifiable integrity guarantees.

**The Role of LIST:** LIST can lead or co-lead technical work on secure and verifiable voting architectures, including validation and auditability frameworks.

### Pillar B. System Integrity Layer: Threat Modelling for Hybrid Scenarios

**The Problem:** Fragmented vulnerabilities across electoral infrastructure, processes, and human interactions can disrupt voting, undermine legitimacy, and increase susceptibility to cyber and hybrid threats.

**The Goal:** Ensuring democratic continuity by identifying and mitigating risks across the electoral lifecycle.

**The Contribution:** A comprehensive electoral threat landscape analysis combining technical, organisational, and human-factor threat modelling. The approach supports election authorities in anticipating vulnerabilities, strengthening operational resilience, and reducing the impact of cyber-enabled

**Uwe Roth**
Luxembourg Institute of Science and Technology
5, avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
uwe.roth@list.lu



manipulation and social engineering, including threat modelling methodologies, risk assessment tools, and crisis simulation scenarios.

**The Technology:** Application of advanced threat modelling methodologies, risk assessment frameworks, and crisis simulation approaches tailored to complex electoral ecosystems.

**The Role of LIST:** LIST can lead or support cross-cutting security and resilience work packages, including systemic risk and hybrid threat assessments.

### Pillar C. Information Integrity Layer: Authenticity and Provenance of Electoral Communications

**The Problem:** Digital dissemination of electoral information enables adversaries to impersonate authorities, manipulate results communication, or distribute forged electoral content, weakening public trust and amplifying disinformation.

**The Goal:** Securing the electoral information supply chain by ensuring that official electoral data and communications are verifiably authentic, tamper-evident, and traceable to trusted sources.

**The Contribution:** A Digital Electoral Information Assurance Layer enabling electoral authorities, observers, media, and civil society to verify the authenticity and integrity of official electoral communications and results dissemination, including authentication frameworks, provenance verification services, and deployment guidelines.

**The Technology:** Deployment of cryptographic authentication mechanisms such as digital signatures, secure timestamping, and tamper-evident publication infrastructures adaptable to different governance and trust models (including transparency logs or distributed ledger technologies where appropriate) to establish verifiable chains of trust.

**The Role of LIST:** LIST can lead or contribute to trusted electoral communication and data provenance components, particularly in authentication and trust verification mechanisms.

## Socio-Technical Integration and Expected Impact

LIST develops cybersecurity solutions that are operationally viable, socially acceptable, and aligned with democratic values. Our work integrates privacy-preserving digital identity approaches, user-centred trust indicators, and transparent security assurance mechanisms , aligning where relevant with European trust service and digital identity frameworks (such as eIDAS) to ensure accessibility, usability, and institutional accountability.

Through these integrity layers, LIST contributes to strengthening public confidence in electoral processes, enhancing resilience against cyber and hybrid threats, and supporting European digital sovereignty through open, auditable, and trustworthy electoral technologies.

LIST aims to act as a trusted technical partner translating democratic principles into deployable and verifiable digital electoral infrastructures.

## The Cybersecurity Group of LIST

The Cybersecurity group of LIST addresses emerging cybersecurity challenges affecting critical infrastructures and digital systems. Its mission is to design and deliver innovative cybersecurity solutions leveraging disruptive technologies while minimizing associated risks. The group operates at the intersection of research, regulation, and innovation, with strong experience in technology transfer and market uptake. Through collaboration with public and private partners, it strengthens digital trust, resilience, and regulatory compliance at European and international levels.

LIST seeks to collaborate with social sciences, legal, governance, and civil society partners to ensure that cybersecurity solutions effectively support democratic participation and institutional trust.