

CyberProtocol AI Trust Standard

A Neutral Global Framework for AI Identity, Provenance, and Compliance Verification

OFFICIAL REFERENCE cyberprotocol.io	SUBMITTED BY One Planet One Earth Foundation Inc.
DATE August 5, 2026	VERSION 1.0, Initial Proposal
DOI 10.5281/zenodo.21803636	

Executive Summary

The world faces a historic moment. Three concurrent developments, EU AI Act enforcement, the founding of WAICO, and the Rome Declaration by Nobel Laureates, all demand verifiable AI. Yet no harmonized, cross-border, cryptographic verification system exists. Governments require it. Businesses cannot comply. Users cannot trust.

The CyberProtocol AI Trust Standard fills this gap. It is an open, neutral, cryptographic framework that verifies who created AI, what it produced, that it is safe, and that it complies with laws, across every border.

This Standard is not controlled by any nation, corporation, or bloc. It is published as a global public good, aligned with United Nations principles. It is designed to be adopted immediately, because the world's laws already require it.

1 The Problem: The Gap

1.1 Three Mandates, No Solution

MANDATE	REQUIREMENT	THE MISSING PIECE
EU AI Act <i>(enforced Aug 2, 2026)</i>	All high-risk AI must carry verifiable proof of origin, safety, and compliance	No harmonized technical standard adopted
WAICO <i>(founded July 16, 2026)</i>	29 nations agree AI governance must be open, inclusive, and verifiable	No verification protocol proposed
Rome Declaration <i>(July 2026)</i>	Nobel Laureates declare AI safety verification a global public good	No working system available to the public

1.2 Why Existing Solutions Fail

APPROACH	CONTROLLED BY	FAILS BECAUSE
Big Tech proprietary systems	US corporations	Antitrust exposure; rejected by other blocs
Nation-state standards	Single governments	Seen as geopolitical tools, rejected abroad
Paper-only guidelines	UN / EU / NIST	No code, no cryptography, no way to actually verify
Human-only identity protocols	Private companies	Do not verify AI agents or AI-generated content

1.3 The Consequence of Inaction

Without a neutral standard:

- **Fragmentation.** Every nation builds its own, producing 10+ incompatible systems and global trade friction.
- **Geopolitical capture.** One bloc's standard dominates, others are excluded, and a digital Iron Curtain forms.
- **Unverifiable AI.** Regulations exist but cannot be enforced, public trust erodes, and technology advances without accountability.

2 The Proposal: Four Pillars

The CyberProtocol Standard is built on four verifiable layers working together as one system. No existing framework covers all four.

Pillar 1: AI & Human Identity

Who or what is acting?

- Decentralized Identifiers (DID) extended for AI agents: `did:cyber:agent`
- **Human identity:** Verifiable Credentials, per W3C standard
- **AI identity:** cryptographic key bound to model, version, and operator

Result: You can distinguish a human from an AI, and know which AI it is, instantly.

Pillar 2: Provenance & Output Certification

Where did this come from?

- Every AI response, file, or transaction carries an immutable cryptographic seal
- Seal includes model ID, timestamp, configuration hash, and operator signature
- **Zero-knowledge option:** prove origin without revealing trade secrets

Result: You can trust what you see, and trace it back to its source, permanently.

Pillar 3: Safety & Risk Compliance

Does this meet legal requirements?

- Standardized compliance metadata maps directly to EU AI Act risk categories
- NIST AI RMF alignment fields included
- ISO/IEC 42001 audit-ready attestation

Result: One proof, recognized by multiple regulatory frameworks simultaneously.

Pillar 4: Cross-Border Verification

Is this proof valid everywhere?

- **Neutral format:** not tied to any nation's signature scheme
- **Recognized by design:** built for UN ECOSOC, EU, WAICO, and Global South adoption
- **Open validation:** anyone can verify the seal, no proprietary software required

Result: One standard, recognized in every jurisdiction, without geopolitical restriction.

3 Design Principles

PRINCIPLE	WHAT IT MEANS
Neutral	No single entity controls the protocol. Governance is multi-stakeholder.
Open	Specification under CC BY 4.0; reference code under Apache 2.0. Free to read, use, and implement.
Interoperable	Built on existing standards (W3C, ISO, NIST), not competing with them.
Privacy-first	Zero-knowledge proofs enable compliance without exposing confidential data.
Permissionless	No gatekeepers. Any AI developer can implement it; any verifier can validate it.

4 Technical Foundation

We are **not** inventing new cryptography. We are **unifying** proven standards into one coherent framework.

LAYER	EXISTING STANDARD	STATUS
Identity	W3C Decentralized Identifiers (DID)	Mature, widely adopted
Credentials	W3C Verifiable Credentials (VC)	Mature, widely adopted
Privacy	Zero-Knowledge Proofs (ZK-SNARKs)	Production-ready
Compliance metadata	Aligned with EU AI Act / NIST AI RMF / ISO 42001	Reference documents exist
Signature	W3C Data Integrity / CBOR signatures	Standardized

The building blocks are ready. No research is needed, only coordination, which we provide.

5 Competitive Landscape

FEATURE	CYBERPROTOCOL	BIG TECH PROPRIETARY	NATIONAL STANDARDS	ACADEMIC PAPERS
Human identity	✓	⬤	⬤	✕
AI agent identity FIRST PROPOSED	✓	✕	✕	✕
AI output provenance	✓	⬤	✕	✕
Cross-border neutrality	✓	✕	✕	⬤
Open & free	✓	✕	⬤	⬤
UN-aligned governance	✓	✕	✕	✕
Ready for immediate use	✓	⬤	✕	✕

✓ Full ⬤ Partial / conditional ✕ Absent

Every competitor builds *pieces*. CyberProtocol is the only framework that connects all four layers into a working system.

6 Publication & Governance Model

ELEMENT	DETAILS
Official reference	cyberprotocol.io
Permanent archive	Zenodo, DOI 10.5281/zenodo.21803636
Technical repository	github.com/ryanpaulpillas/cyberprotocol-ai-trust-standard, open-source reference implementation
Stewardship	One Planet One Earth Foundation Inc., holder of UN ECOSOC Special Consultative Status since 2025
Standard license	Creative Commons Attribution 4.0 International (CC BY 4.0), free in perpetuity
Code license	Apache 2.0, permissive, commercial use allowed
Commercial implementation	Available via certified partners; the standard itself remains a public good

7 Call to Action

To the United Nations & Member States. Recognize cyberprotocol.io as a reference framework for AI verification. It is open, neutral, and ready. Delay means fragmentation, higher costs, and less safety. Adopt one standard and make it available to all nations equally.

To AI developers. Implement the Standard. It is free, it is open, and verification obligations are already entering law. Building it in now saves rework later.

To the global public. Demand verifiable AI. When you cannot tell whether content is human or machine-generated, democratic discourse is at risk. CyberProtocol restores transparency.

8 Timeline & Next Steps

PHASE	MILESTONE
August 2026	Standard proposed to UN ECOSOC · Published to Zenodo & GitHub
Q4 2026	First reference implementation · Pilot integrations with AI labs
2027	Formal adoption by nations · Integration into regulatory enforcement
2028+	Global default: every AI output carries a CyberProtocol seal

9 Conclusion

The laws of the world have already spoken. They demand AI that is verifiable, safe, and accountable. What remains is the technical instrument to make those laws work.

The CyberProtocol AI Trust Standard is that instrument. It requires no new invention, only the decision to build one system that serves everyone, rather than a few.

We propose it now, not as a commercial product, but as a global public good, at **cyberprotocol.io**.

Support this work

The CyberProtocol Standard is a global public good, free to all in perpetuity. Advancing it to a working reference implementation, pilot integrations with AI laboratories, and neutral multi-stakeholder governance requires support. Funders, philanthropies, standards bodies, and industry partners are invited to help build the trust layer of the AI era. Contributions are stewarded by One Planet One Earth Foundation Inc., holder of UN ECOSOC Special Consultative Status since 2025.

[Partner with us](#)