Yaoundé, 31th July 2025

To: Kluz Prize for PeaceTech
Kluz Center for Tech Diplomacy
info@kluzprize.org

Ref. 036/2025
Subject: Covert Letter – SUR Project Submission

To the Kluz Prize for PeaceTech Committee,

We are honored to submit our project entitled **The SUR Infrastructure: Ubuntu-Informed Cryptography for Relational Protection of Unaccompanied Minors Refugee Data**, for consideration for the 2025 Kluz Prize for PeaceTech.

SUR is a cryptographic infrastructure specifically designed to protect the data and dignity of unaccompanied refugee minors. Rooted in African ethical principles such as **Ubuntu, Adna** and in recent advances in theoretical cryptography (developed at the National Advanced School of Engineering of Yaoundé), SUR proposes a modular architecture, Iron, Gold, and Clay layers, to ensure time-stamped, legally interpretable, and semantically coherent protection of sensitive data.

Our system is based on the Q2CSI framework, which has been developed and is available on ePrint. However, SUR is fully self-contained and understandable without prior knowledge of that foundation. The current version includes a formal description, security models, and a prototype roadmap. The submitted material summarizes the infrastructure, the real-world context of application, and the technical and ethical contributions of the project.

Should we be selected, the prize would allow us to develop a functional prototype in collaboration with humanitarian actors and field-based NGOs. This implementation would integrate real-world cryptographic primitives (post-

quantum and conventional), adapted to the specific constraints of local partners, while preserving the explainable guarantees defined at the theoretical level.

The material (archive) is made of:

- Mariam's_Case.pdf: exposes a real-world scenario illustrating how SUR protects unaccompanied minors like Mariam across six humanitarian contexts, translating ethics into verifiable protection through layered cryptography.
- SUR_Core_Crypto.pdf: supports scientific rigor, we include a standalone technical document detailing SUR's cryptographic architecture, formal definitions, security proofs, and post-quantum resilience under the CRO trilemma model.
- The_SUR_Project.pdf : provides a concise project overview highlighting SUR's ethical and cryptographic foundations, its alignment with the Q2CSI model, and its unique position as a civiltech innovation rooted in Ubuntu and Adna principles.
- Kinship_hash.py: depicts a dedicated kinship hash module illustrates how SUR encodes relational identities (tribe, clan, fictive kin) in a culturally faithful, post-quantum resistant format
- Dataset.json: is a structured dataset simulating 20 diverse unaccompanied minors, across regions and genders, for cryptographic protection testing and social inclusion modeling
- Mariam's_PoC.py: demonstrates SUR's real-world operability, we provide a minimal but complete contextual hashing prototype that generates and verifies Mariam's signature under Q2CSI semantics.

Thank you for considering our submission.

Sincerely,

Thierry Emmanuel MINKA MI NGUIDJOI

AfroLeadership – Research Director

thierry@afroleadership.org