Project Charter: Trusted Transaction Assurance Working Group

1. Vision & Mission

Vision: To enable a secure, interoperable, and transparent digital ecosystem where any organization can confidently verify identity and authorize critical digital actions and records with the highest level of integrity.

Mission: This working group will bridge the critical gaps between identity proofing and authorization. We will foster a clear, component-based marketplace for identity services and establish the definitive standards for binding verified digital identities to legally enforceable and significant actions.

2. Problem Statement & Opportunity

The digital identity landscape is at a pivotal moment. The release of NIST SP 800-63 v4 provides a modern, modular framework for identity proofing, and Kantara's US Assurance Program is poised to develop the corresponding assessment criteria. While these developments are foundational, they leave critical market-level and downstream challenges unaddressed:

- **Persistent Market Confusion:** Relying Parties (e.g., banks, healthcare providers) are confronted with a confusing array of certifications (FRTE, RIVTD, etc.) and vendor claims of "NIST compliance" that are difficult to verify and translate into practical risk management decisions.
- **Component Integration Friction:** Credential Service Providers (CSPs) lack a streamlined way to discover, integrate, and demonstrate compliance for best-in-class, pre-certified identity components (e.g., document liveness, biometric matching), leading to costly and redundant monolithic assessments.
- **The Authorization Gap:** A verified identity at enrollment is not the same as an authorized action later. The industry lacks a standardized, high-assurance method for binding a verified identity to a specific digital event, such as signing a mortgage, granting durable consent for care, or approving a wire transfer. This gap is a primary vector for sophisticated fraud and critical errors.

This working group will address these challenges directly, creating the market-enabling frameworks necessary to unlock the full potential of a componentized, high-assurance identity ecosystem.

3. Business Case

By solving these problems, this working group will deliver significant value to the entire digital economy:

- **Accelerate Adoption:** A transparent marketplace for certified identity components will reduce friction for both builders (CSPs) and buyers (RPs), accelerating the adoption of secure identity solutions.
- **Reduce Fraud and Error:** Establishing a standard for binding identity to actions will directly combat fraud and reduce critical errors in the multi-trillion dollar markets for financial services, healthcare, real estate, and legal transactions, for a more secure and interoperable digital trust ecosystem.
- **Foster Innovation and Specialization:** Enabling a "plug-and-play" model for identity components will foster a competitive market where specialized vendors can deliver best-in-class solutions, improving quality and reducing costs.

4. Primary Objectives & Workstreams

This group's work will be organized into two primary, parallel workstreams:

Workstream A: Identity Component Marketplace Enablement

This workstream will focus on creating the tools for a transparent and efficient marketplace for identity proofing components, serving as a vital partner to the Kantara US Assurance Program.

- **Objective A1: Develop the "Micro Trust Mark" Registry Framework.** Define the conceptual model and data schema for a public registry of certified identity components. This registry will serve as a "single source of truth" for the industry.
- **Objective A2: Create a Market Translation Layer.** Develop clear, business-friendly guidance that maps different assessment programs (e.g., Kantara's future criteria, FRTE, RIVTD) to the functional requirements of NIST SP 800-63A-4, enabling Relying Parties to make informed risk decisions.
- **Objective A3: Define a Consumption Model for External Testing Results.** Establish a standardized process for how the registry can ingest, verify, and display certifications from other accredited labs and conformity assessment bodies.

Workstream B: High-Assurance Action & Record Binding Standards

This workstream will address the critical gap between proofing and authorization, establishing the next frontier of digital trust.

- **Objective B1: Define Standards for Identity-Bound Actions & Records.** Develop the technical and policy framework for binding a verified digital identity (at IAL2 and above) to a digital record or action, creating a verifiable, non-repudiable "Identity-Signed Record."
- **Objective B2: Target High-Stakes Use Cases.** Initially focus on the requirements for critical interactions across regulated industries, including verifiable patient consents, secure e-prescribing, high-assurance electronic signatures, and high-value payment authorizations.
- **Objective B3: Foster Cross-Industry Collaboration.** Actively partner with adjacent industry organizations, such as the Electronic Signature and Records Association

(ESRA) and key healthcare standards bodies such as HL7, to ensure standards are legally sound, technically robust, and meet market needs.

5. Scope & Deliverables

In Scope:

- Developing frameworks, data models, and best-practice guides.
- Publishing whitepapers and recommendations.
- Facilitating industry-wide collaboration and proofs-of-concept.
- Providing market requirements and feedback to conformity assessment bodies like the Kantara US Assurance Program.

Out of Scope:

- Operating as a conformity assessment body or testing lab.
- Developing and maintaining its own proprietary assessment criteria for identity proofing components (this is the role of the Kantara US Assurance Program).

Initial Deliverables:

1. A whitepaper defining the "Micro Trust Mark" Registry Framework.
2. A draft standard for creating an "Identity-Signed Record" for high-assurance digital consent and signatures.
3. A market guide translating existing identity testing programs for Relying Parties.