Public Architecture Blueprint: Jill.ai & IOkT (Public Edition)

Strategic Hierarchy

Parent Entity: Jill.ai (The Innovation Lab)

- **Mission**: Intelligence with Integrity
- **Brand Positioning**: "Jill of all Trades" - representing versatility, problem-solving, and operational excellence
- **Future Roadmap**: "Project Uplift" (AI Career Mentorship platform)

Flagship Product: IOkT (Internet of Kids' Things)

- **Mission**: The "SSL Layer" for Child Safety
- **Positioning**: The fundamental safety infrastructure that should exist by default on the internet

---

The Founder Story ("User Zero")

Estelle Coetzee is a self-taught Full-Stack Developer and Operations Veteran with experience in Power Stations and Hazardous Locations. She built IOkT because existing market solutions failed her neurodiverse daughter (10) and her son (20). She has personally witnessed the harm the internet causes, even to adults.

Estelle represents the "Jill of all Trades" archetype:

- **Grit**: Solo founder navigating pre-seed challenges
- **Resilience**: Building through personal adversity (MOFO resilient)
- **Operational Excellence**: Bringing industrial safety mindset to digital child protection
- **Technical Versatility**: AI Generalist path as a specialization

This personal connection to the problem drives IOkT's uncompromising focus on child safety and privacy.

Future Pipeline: Project Uplift

Vision Statement

Project Uplift is Jill.ai's next social impact initiative—an AI-powered career mentorship platform designed to democratize access to professional guidance for youth entering the workforce.

Core Mission

Just as IOkT protects children online, Project Uplift empowers young adults transitioning into careers. It addresses the "digital divide" in professional development, where access to quality mentorship often depends on socioeconomic status or geographic location.

Target Audience

- **Primary**: Unemployed job seekers or career changers seeking guidance in emerging tech fields
- **Secondary**: Youth aged 16-24 in underserved communities (Global South focus)
- **Distribution**: Schools, community colleges, job centers, NGO partnerships

Planned Features

- **AI Career Coach**: Personalized mentorship using LLM-powered guidance tailored to individual career paths
- **Resume & Portfolio Builder**: AI-assisted tools to help youth create professional materials
- **Interview Preparation**: Mock interview practice with real-time feedback and coaching
- **Skills Gap Analysis**: Identify market-demanded skills and create personalized learning roadmaps

- **Job Matching**: Connect youth with opportunities aligned to their skills and aspirations
- **Mentor Matching**: Pair users with human mentors in their fields of interest
- **Community Support**: Peer learning groups and success story sharing

Technology Approach

The platform will leverage the same agent framework developed for internal operations (LangGraph + LlamaIndex + FastAPI), demonstrating Jill.ai's ability to deploy versatile AI solutions across multiple social impact domains.

Development Status

- **Current Phase**: Concept development and demand validation
- **Timeline**: Post-IOkT MVP launch (Phase 3+)
- **Target Impact**: 10,000+ job seekers mentored in first 18 months

---

IOkT Master Architecture Overview

The Internet of Kids' Things

Vision Statement

Building the infrastructure to transform the internet from an open bar into a curated, safe environment for children—using AI as a guardian and Web3 for verifiable child identity and data ownership.

Core Mission

If the internet were built today with the knowledge we now have about child safety, it would look like IOkT. We're building the infrastructure that should have existed from the beginning.

Product Overview

The IOkT Suite includes IOkT ID Secure, IOkT Net, IOkT Key, and **IOkT Tutor** (the guided learning / social hub layer).

Target Market: The Grey Market

- **Primary**: Global South (Android/Huawei dominant)
- **Distribution**: Schools, community groups, B2B "Compliance-as-a-Service" API
- **Market Gap**: Current age-gates and COPPA protections are checkbox failures

The Three-Phase Evolution

Phase 1: The Shield (Months 1–6)

- Android-first MVP with Neural Keyboard safety agent
- Safe Browser (Chromium fork with Safety DNS)
- Local AI processing for privacy
- Parent verification via MaxMind minFraud

Phase 2: The Key (Months 7–12)

- iOS support via VPN Profile & Safari Extension (DNS)
- "Login with IOkT" for VIP partner rewards
- Partnerships with indie game developers
- Enhanced identity verification (Polygon ID/Verifiable Credentials)

Phase 3: The World (Year 2+)

- Social Hub for verified children
- DAO/community moderation
- Cross-platform credential portability
- Full decentralized governance model

Technical Architecture Stack

The "Android Guardian" MVP Specification

Platform Strategy: Android First

- **Distribution**: Google Play Store & Huawei AppGallery
- **Rationale**: Grey Market dominance, deep system integration capabilities

- **Timeline**: Phase 1 (Months 1-6)

Core Components:

1. The Neural Keyboard (The Bouncer)

- **Function**: Replaces the default Android keyboard, travels into encrypted apps (WhatsApp, TikTok, Snapchat)
- **Technology**: On-Device TinyML using TensorFlow Lite
- **Capabilities**:
  - Sentiment analysis in real-time
  - Grooming pattern detection
  - PII sharing prevention
  - Contextual coaching ("Are you sure you want to say that?")
- **Privacy**: All processing happens locally on device, zero data transmission
- **Performance**: Optimized for low latency to maintain natural typing experience

2. The Safe Browser

- **Function**: Chromium fork with built-in safety features
- **Technology**: Hard-coded DNS filtering for Red Zone domains
- **Protection Layers**:
  - Porn/gambling domain blocking
  - Malware site prevention
  - Phishing protection
  - Safe Browsing API integration
- **Parent Controls**: Whitelist/blacklist customization

3. The Biometric Handshake (Zero-Trust Login)

- **Function**: Identity verification and credential issuance
- **Flow**:
  1. Parent verifies identity (biometric + MaxMind minFraud)
  2. Parent issues Child Credential (Verifiable Credential)

3. Child authenticates via device biometrics

- **Security**: Zero-knowledge proof of age/consent without exposing PII

Mobile Platform

- **Primary**: Native Android (Kotlin) for deep system integration
- **Keyboard/Launcher**: Custom implementations for safety layer
- **Future**: iOS via VPN Profile & Safari Extension (DNS)

AI Safety Layer ("The Bouncer")

Component	Technology	Purpose
On-Device NLP	TFLite (quantized BERT/MobileBERT)	Real-time content analysis for grooming, bullying, PII
Local LLM	TinyLlama/Phi-3	Contextual guidance and "Red Zone" content blocking
Safety DNS	Custom DNS resolver	Network-level filtering and Safe Browsing integration
Neural Keyboard	Client-side NLP	Pre-send analysis of all typed content

Identity & Verification ("The Passport")

Parental Verification Stack:

- **MaxMind minFraud API**: Risk scoring for parent identity verification
  - Cross-network reputation analysis
  - Velocity checks (email, IP, billing patterns)
  - Geolocation mismatch detection
  - Proxy/VPN detection
  - Shared fraud intelligence from thousands of businesses

Child Identity Framework:

- **Initial**: Parental Attestation model
- **Roadmap**: Polygon ID Verifiable Credentials (W3C standard)
- **Long-term**: Soulbound Tokens (SBTs) on Layer 2 blockchain

Credential Architecture:

- Verifiable Credentials for age-gating
- Parental consent workflows
- Zero-knowledge proofs for selective disclosure
- Privacy-first: prove "over 13" without revealing birthdate

Backend Infrastructure

Cloud Services:

- **Primary**: Huawei Cloud (aligned with Grey Market strategy)
- **Fallback**: Firebase/Firestore for real-time data
- **Notifications**: WhatsApp Business Cloud API for parent alerts

Storage Strategy:

- **On-Chain**: Credential hashes, revocation lists, access tokens
- **Off-Chain Encrypted**: Personal data, educational records, chat history
- **Decentralized**: IPFS/Arweave for permanent credential anchoring

---

Blockchain Platform Strategy

SELECTED NETWORK: Polygon (zkEVM / PoS)

Decision Rationale:

- **Ecosystem Maturity**: Largest EVM-compatible developer ecosystem with battle-tested tools
- **Account Abstraction Support**: Leading implementation of ERC-4337 for gasless transactions and parent-managed accounts
- **Zero-Knowledge Privacy**: Polygon ID (Privado ID) provides W3C Verifiable Credentials with ZK-proofs
- **Cost Efficiency**: Sub-cent transactions enable sustainable "free for kids" model
- **Best Overall Fit**: Highest weighted score (9.1/10) across all critical IOkT requirements

Selected Components:

Identity Protocol: Privado ID (Polygon ID)

- W3C-compliant Verifiable Credentials
- Zero-knowledge proof generation for selective disclosure
- Age verification without revealing birthdate
- Parental consent workflows built-in

Token Standard: Soulbound Tokens (SBTs)

- Non-transferable "Digital Citizenship" badges
- Educational achievement credentials
- Access tokens bound to child identity
- ERC-5192/ERC-721 extensions for enforcement

Wallet UX: Account Abstraction (ERC-4337)

- Gasless transactions sponsored by platform
- Social recovery via parent guardian keys
- Session keys for limited permissions
- No seed phrases required for children
- Biometric authentication (device-native)

Recommended Multi-Layer Architecture

Identity & Credential Layer:

- **Primary Choice**: Polygon zkEVM + Polygon ID (Privado ID)
- **Alternative**: Algorand (strong SSI support) or cheqd (identity-first)
- **Rationale**: Mature VC/SSI tooling, W3C standards compliance, ZK-proofs for privacy

Transactional Layer (High-Volume Actions):

- **Primary**: Polygon PoS for cost-efficiency
- **Alternative**: Solana for extreme throughput, Sui for object-centric model
- **Purpose**: Badge minting, status updates, micro-transactions

Privacy/Guardian Layer:

- **Long-term**: Internet Computer Protocol (ICP)

- **Features**: Reverse gas model (developer pays), Internet Identity, full-stack on-chain
- **Purpose**: Guardian AI processing, private computation

Audit & Compliance Layer:

- **Optional**: Hedera Hashgraph for timestamping
- **Purpose**: Regulatory audit trails, immutable compliance records

---

Safety Architecture: Multi-Layered Approach

Layer 1: Device-Level Protection

- Neural Keyboard intercepts all typing
- Local AI analysis before transmission
- Safe Browser with DNS filtering
- No data leaves device until verified safe

Layer 2: Network-Level Filtering

- Safety DNS blocks known harmful domains
- Real-time threat intelligence updates
- Parent-controlled whitelist/blacklist
- Regional content filtering

Layer 3: Identity & Access Control

- Age verification via Verifiable Credentials
- Parental consent required for all actions
- Time-based access controls
- Platform-level age-gating

Layer 4: Behavioral Analysis

- Pattern recognition for grooming attempts
- Sentiment analysis for cyberbullying
- PII leakage detection

- Automated parent alerts for high-risk scenarios

Layer 5: Community & Governance

- Peer reporting mechanisms
- DAO-based content moderation (Phase 3)
- Transparent decision-making
- Appeals process for false positives

Regulatory Compliance Framework

Privacy Regulations

- **COPPA (US)**: Verifiable parental consent, data minimization
- **GDPR-K (EU)**: Right to erasure, data portability, privacy by design
- **POPIA (South Africa)**: Lawful processing, security safeguards

Compliance Design Patterns

- Off-chain storage for PII (encrypted)
- On-chain only: hashes, revocation lists, access proofs
- Selective disclosure via ZK-proofs
- Parental consent workflows with audit trails
- Age-appropriate data retention policies

Pilot Program Overview

Value Proposition

"Give your child a safer digital experience over the December holidays when screen time peaks and parental supervision is harder."

Pilot Timeline

- **Recruitment**: November 2024
- **Onboarding**: Early December 2024

- **Active Pilot**: December 2024 - January 2025 (holiday period + back-to-school)
- **Feedback Collection**: January 2025

Success Criteria

- **80%+ retention** through pilot period
- **Parent NPS >70**: Would recommend to other parents
- **99.9% Block Rate for Red Zone content**: Statistically robust safety performance
- **Technical stability**: <1% crash rate, <5% battery drain increase

---

Terminology & Concepts

Digital Seatbelt: The fundamental safety layer that should exist by default

Grey Market: Global South regions with Android/Huawei dominance

Passport & Bouncer: Identity verification + content filtering agents

Shield/Key/World: The three-phase product evolution

Login with IOkT: OAuth-style authentication for partner platforms

Safety DNS: Custom DNS resolver for network-level protection

Red Zone: Content categorized as dangerous/inappropriate for children

---

Next Steps for AI Agent Integration

1. **Agent Registry**: Build centralized directory of all IOkT safety agents
2. **Workflow Engine**: Define multi-agent processes for threat detection and response
3. **Intelligence Layer**: Implement federated learning for improved content detection
4. **Guardian AI**: Deploy privacy-preserving AI on ICP for sensitive processing
5. **Governance Framework**: Establish policies for agent communication and escalation