ENTICARD & ENTIFONE SYSTEM WHITEPAPER

Dual-Device Cryptographic Architecture for a Trust-Guaranteed Digital Life

1. Introduction

The ENTIFY ecosystem is built on the premise that digital identity must be anchored in physical reality, supported by verifiable assets, accountable reputation, and a provable chain of custody for all actions.

To achieve this securely for billions of non-technical users, ENTIFY introduces a dual-device architecture:

- EntiPhone → the daily-use smart device, optimized for convenience, communication, secure transactions, and identity presence in the network.
- EntiCard → an offline-secure, tamper-resistant hardware module containing the master identity seed, serving as the cryptographic fallback and ultimate recovery mechanism.

Together they form the world's most secure personal identity system:
A hot device for daily operations + a cold device for immutable personal sovereignty.

2. System Overview

EntiPhone: The Active Identity Node

A secure smartphone-like device running EntiOS with:

- Real-time identity verification
- Encrypted P2P communication
- Zero-knowledge authentication for apps and services
- Secure biometric or passphrase wallets
- Local execution of Proof-of-Humanity protocols
- Secure signing for micro-transactions
- Direct participation in ENTIFY's Trust Graph consensus

The EntiPhone is always online, always authenticated, always accountable.

EntiCard: The Deep Cold Identity Module

A credit-card-sized secure element containing:

- Master Identity Key (MIK)
- Cryptographic seeds for all EntiPhone derivation keys
- Air-gapped hardware signing capability
- No OS, no UI, no wireless communication
- Designed to survive for decades
- Used only for rare events: recovery, identity rotation, inheritance, catastrophic compromise response.

The EntiCard is never online.
It maintains zero attack surface.

3. Cryptographic Architecture

3.1 Identity Key Hierarchy

Master Identity Key (MIK) — stored ONLY in EntiCard
|
|-> Device Keys (EntiPhone, EntiPad, etc.)
|-> Financial Keys (EnToken Wallet)
|-> Reputation Keys
|-> Messaging Keys
|-> Multi-Party Recovery Keys

EntiPhone Derivation

The EntiPhone derives time-rotating subkeys using:

- HKDF with rotation intervals
- Physical sensor entropy
- Secure enclave counter seeds
- EntiNet trust attestation

Result: Even if an attacker steals the EntiPhone, they cannot derive the identity root.

EntiCard Signing Mode

The EntiCard only performs:

- Identity reinstatement

- Device authorization
- Master key rotation
- High-value asset claims
- Unique biometric seed resets

No other operations are allowed.
The card cannot broadcast, cannot connect, cannot leak.

4. Security Model

4.1 Threat Surfaces

ENTIFY's dual-device model neutralizes:

Threat	Mitigation
Phone theft	Identity cannot be extracted without EntiCard
Malware on device	Keys are non-exportable; transactions are ZK validated
Coercion	EntiCard supports hidden "duress keys"
Cloud breaches	No master key ever leaves the card
Government overreach	Keys cannot be compelled from ENTIFY—users hold sovereignty
Supply chain attacks	EntiCard performs self-attestation of secure element integrity

4.2 Multi-Layer Authentication

EntiPhone Authentication Stack

1. Local biometrics (private; never shared)
2. Device integrity attestation (TEE)
3. ZK Proof of Identity Continuity
4. Cryptographic challenge-response with Trust Graph validators

EntiCard Authentication Stack

1. PIN or passphrase entry
2. Card activates secure signing mode
3. One-time relay via NFC/USB to device
4. Immediately powers down

The card is offline before and after all operations.

5. Network Functionality Enabled by Both Devices

5.1 User Identity Lifetime

Stage	EntiPhone	EntiCard
Onboarding	Trusted onboarding, biometric capture, live-proof	Stores MIK securely
Daily Use	Messaging, payments, commitments,	Unused
Lost / Replace	Initiates recovery process	Authenticates new device
High-Value Operations	Signs with subkeys	Confirms root-level authorizations
Emergency	Triggered via app or remote call	Restores identity or rotates

6. Interaction Workflow

6.1 New User Onboarding

1. User receives EntiPhone + EntiCard kit
2. EntiPhone creates derived daily-use keys
3. EntiCard generates MIK internally
4. EntiPhone receives derived keys from card via one-time setup
5. MIK is permanently sealed in the card

At no time is the MIK revealed to any software.

6.2 Daily Use Case Example

- Logging into an app
- Signing a transaction
- Sending an authenticated message
- Confirming work performed
- Managing assets or insurance claims

All performed by EntiPhone with no involvement from the card.

6.3 Lost EntiPhone Scenario

User retrieves EntiCard from safe place:

1. Buy new EntiPhone or EntiPhone replacement module
2. Card authorizes new device
3. Trust Graph validators confirm continuity of identity
4. Old device is cryptographically revoked
5. Derived keys regenerated

Recovery completed with no central authority.

6.4 Lost EntiCard Scenario

Because card loss is more serious, ENTIFY design allows:

- Multi-party backup split keys
- Validator-based recovery system
- Inheritance protocols
- Delayed-time recovery locks (e.g., 14 days)

No single party can replace the card without consensus.

7. EntiPhone Capabilities in Detail

7.1 Secure Computing Stack

- Custom hardened OS
- Layered sandboxes
- Rust-first runtime
- Permissionless P2P networking
- Integrated end-to-end encrypted apps

7.2 Built-In Service Modules

- Wallet + EnToken gold-backed settlement

- Reputation scoring
- Real-world asset tokenization
- Insurance pool claims
- Identity proof marketplace
- Work marketplace integration
- Decentralized telecom relay identity (EntiMesh)

8. EntiCard Hardware Architecture

8.1 Physical Specifications

- Secure element: EAL7+
- Passive power via NFC
- Optional micro-battery under duress-mode
- 30-year key material durability
- Epoxy-filled, laser-etched, tamper-resistant body
- Self-destruct fuse if invasive reading is attempted

8.2 Supported Functions

- Generate MIK
- Authorize new devices
- Rotate entire key hierarchy
- Approve asset-backed token minting
- Approve asset redemption
- Approve major insurance claims
- Trigger identity lockout
- Enable legacy/inheritance protocol

9. Design Philosophy

The EntiPhone = convenience

The EntiCard = sovereignty

This mirrors real-world security:

- Phone = your wallet
- Card = your vault key

Users operate safely knowing that even catastrophic compromise can be reversed.

10. Why Two Devices Are Necessary

Single-device identity systems fail due to:

- Software exploits
- Zero-day vulnerabilities
- User error
- Physical theft
- Coercion
- Remote malware insertion
- Compromised supply chains

Dual-device gives ENTIFY:

- Cold + hot security model
- Irreversible proof of ownership
- Cryptographic disaster recovery
- Guaranteed continuity for real-world assets
- Confidence for large institutions
- Self-sovereignty with no central authority

11. System Benefits

To Individuals

- Maximum security for identity + assets
- Convenient daily usability

- Peace of mind through recoverability
- Protection from fraud, coercion, and impersonation

To Enterprises

- Verifiable identity relationships
- Cryptographically guaranteed workforce management
- Asset tokenization at zero trust cost
- Insurance-backed transactions

To Governments

- Fraud reduction
- Non-intrusive verification
- Optional compliance layers

12. Conclusion

The EntiCard + EntiPhone architecture is the cornerstone of ENTIFY’s mission:

To make digital identity, ownership, and communication trustworthy again — permanently and globally.

By separating daily-use cryptographic operations from deep cold identity storage, ENTIFY becomes the first decentralized system robust enough for real-world identity, yet simple enough for billions of users.