Kore
Inside

KoreID Individual, KoreID Entity, KYT and KYA

KoreID

Identity, Authority, and Transaction-Grade Trust for Regulated Markets

Regulated financial markets require more than trust. They require provable identity, verifiable assets, and defensible transactions. KoreID provides foundational trust infrastructure for compliant participation across regulated private and capital markets by unifying four integrated layers: KoreID Individual, KoreID Entity, Know Your Asset (KYA), and Know Your Transaction (KYT).

KoreID Individual — Natural Person Identity (KYC)

KoreID Individual establishes the verified identity, eligibility, and authority of natural persons participating in regulated transactions. It integrates identity verification, AML and sanctions screening, suitability determination, authentication and authorization, and verified wallet ownership into a continuously monitored financial identity passport. This layer ensures individuals remain eligible and authorized to act at the moment an action occurs.

KoreID Entity — Organizational Identity (KYB)

KoreID Entity establishes the verified identity, legal existence, and authority of organizations participating in regulated markets. It validates corporate status, ownership and control, authorized signatories, regulatory standing, and ongoing eligibility, ensuring entities are properly constituted and empowered to transact under applicable jurisdictional requirements.

Know Your Asset (KYA) — Verifiable Asset Identity

Know Your Asset (KYA) establishes a verifiable and auditable identity for the asset itself. KYA attests to the asset's type, class, quantity, rights, restrictions, provenance, and regulatory characteristics across securities, real-world assets, and digital representations. This layer ensures that what is being transacted is precisely defined, legally recognizable, and compliant, whether at rest or in motion.

Know Your Transaction (KYT) — Transaction-Grade Assurance

Know Your Transaction (KYT) proves that a specific transaction was lawful, authorized, and compliant at the moment it occurred. KYT binds verified individuals, entities, and assets to applicable regulations, required disclosures, attestations, consent, and provable execution. KYT is not a standalone check—it is the outcome of KoreID Individual, KoreID Entity, and KYA operating together.

The KoreID Trust Model

KoreID Individual verifies people. KoreID Entity verifies organizations. KYA verifies assets. KYT proves the transaction itself. Together, these layers transform fragmented compliance processes into a continuous, transaction-grade trust framework designed for auditability, enforceability, and scale.

KoreID
Individual
The Financial Markets Identity & Compliance Passport

A continuously monitored, reusable trust layer for regulated private and capital markets.

What KoreID Is

KoreID is a market-grade digital identity passport built specifically for regulated financial markets. It unifies, in one system:

- Identity Verification
- AML Risk Controls
- Sanction Screening
- Suitability & Eligibility
- Login, Authentication, Authorization
- Verified Public Wallet Addresses
- Continuous Monitoring (not a one-time "whitelist")

Analogy: TSA PreCheck + Global Entry + Schengen Passport for the global financial markets.

Why KoreID Exists

Most "digital identity" solutions solve only a fraction of the problem (login or KYC or wallet identity). In regulated markets, identity must answer, continuously, provably, and defensibly, the following questions:

- Who are you?
- Are you eligible to participate right now?
- Are you authorized to perform this specific action?
- Is this wallet address truly yours and still valid?
- Are there new risks that require restriction, review, or revocation?

Static checks and point-in-time onboarding do not meet real market requirements.

What Makes KoreID Different

1) Full-Stack Identity + Compliance + Permissions

KoreID integrates identity proofing, compliance screening, eligibility, and authorization into a single reusable passport, reducing vendor sprawl and integration complexity.

2) Continuous Monitoring (Living Passport)

KoreID continuously evaluates risk and eligibility across the user lifecycle: sanctions updates, AML risk changes, adverse events, suitability changes, and wallet changes, supporting restriction, revocation, and re-approval workflows.

3) Transaction-Grade Authorization

KoreID governs what a user is allowed to do at the moment of action by role, policy, jurisdiction, and rule-based controls.

4) Verified Public Wallet Addresses

KoreID treats wallet addresses as regulated identity artifacts: ownership attestation, lifecycle controls, change management, and audit-ready provenance.

5) Ecosystem Passporting

Users can onboard once and reuse KoreID across participating issuers, marketplaces, broker-dealers, transfer agents, and partners, subject to consent, governance, and data-sharing agreements.

Business Outcomes

For investors: Faster onboarding, less repetition, higher trust.

For issuers & platforms: Higher conversion, lower compliance friction, consistent enforcement.

For regulated intermediaries: Continuous risk controls, defensible audit trails, revocation and re-approval clarity.

KoreID is a continuously monitored financial identity and compliance passport, enabling secure, compliant participation across regulated markets.

KoreID Entity

Verifiable Business Identity for Regulated Private Markets

Private capital markets do not operate on trust in individuals alone. They operate on trust in legal entities such as companies, intermediaries, and regulated firms, whose authority to act is defined by corporate law, licensing regimes, and regulatory oversight.

KoreID Entity is Kore's solution for establishing and governing that trust.

While **KoreID Individual** verifies natural persons, **KoreID Entity** verifies the business entity itself: its legal existence, operational legitimacy, regulatory authorization, and ongoing standing. Together, they form a complete identity and compliance layer for private markets.

Why Entity Identity Matters

Most failures in private-market compliance do not stem from bad actors impersonating people. They stem from:

- Entities operating outside their authorized scope
- Lapsed licenses or registrations
- Unclear authority to bind the entity
- Changes in control or standing that go undetected

Traditional KYB is typically fragmented, point-in-time, and disconnected from transaction systems. KoreID Entity replaces that model with a persistent, governed entity identity that is embedded directly into market infrastructure.

What KoreID Entity Establishes

KoreID Entity provides authoritative answers to the questions that regulators, platforms, and counterparties must be able to rely on:

- Is this a real, legally formed organization?
- Is it active and in good standing?
- Is it authorized to operate in its claimed role?
- Who controls it and who may act on its behalf?
- Does it remain compliant over time?

These assurances are not static attestations. They are continuously maintained within Kore's compliance framework.

The Common KYB Foundation

Every organization entering the Kore ecosystem is anchored to a common KYB foundation, regardless of industry or role.

Legal Identity and Formation

KoreID Entity verifies the entity's legal formation, jurisdiction, registration details, and operating addresses. Trade names and DBAs are linked to the canonical legal entity to preserve referential integrity across systems.

Corporate and Tax Identifiers

Corporate identifiers such as EIN/TIN (or jurisdictional equivalents) are validated and reconciled against authoritative records, ensuring the entity can be uniquely and reliably identified.

Good Standing

The entity's current legal status is confirmed to ensure it is active and not dissolved, suspended, or administratively restricted. Where applicable, formal good-standing attestations are validated.

Ownership, Control, and Authority

KoreID Entity establishes who controls the organization and who is authorized to act on its behalf. Officers, directors, managers, and authorized signers are identified, creating a clear and auditable chain of authority for contractual and transactional actions.

License Determination

KoreID Entity evaluates whether the entity's activities require licenses and captures the relevant license information when required. This ensures that authorization is tied to actual business function, not just entity type.

Risk and Compliance Screening

At the entity level, KoreID Entity performs sanctions and watchlist screening and applies ongoing monitoring so changes in risk posture, status, or eligibility can be detected and governed.

This baseline KYB layer applies universally—issuers, service providers, and intermediaries alike.

Role-Based KYB: Authorization by Function

Beyond the common foundation, KoreID Entity applies role-specific verification based on what the organization claims to be—and what it seeks to do in the market.

Operating Companies

For issuers and general operating businesses, KoreID Entity confirms corporate legitimacy, governance structure, and authority to transact. This ensures that companies raising capital or participating in private transactions are legally capable of entering enforceable agreements and fulfilling their obligations.

Regulated Market Participants

For regulated entities, KoreID Entity extends beyond corporate KYB into regulatory authorization and scope validation.

- **Broker-Dealers:** Verified through CRD numbers and SEC registrations to ensure authorization to perform broker-dealer functions relevant to the transaction.
- **Audit Firms:** Verified via **PCAOB registration**, confirming eligibility to perform audits in regulated capital-market contexts.
- **Alternative Trading Systems (ATS):** Verified by confirming that ATS operations are supported by appropriately licensed broker-dealers and aligned with applicable regulatory permissions.
- **Transfer Agents:** Verified through SEC registration, confirming authority to perform issuance, recordkeeping, and transfer functions.

For each regulated role, KoreID Entity validates not just identity, but permission, scope, and standing, and continuously monitors those attributes.

Continuous Monitoring, Embedded Governance

KoreID Entity is designed for continuous assurance, not episodic checks.

Changes in corporate status, regulatory standing, license validity, or control structure can automatically influence permissions, access rights, and workflow eligibility across the Kore ecosystem. Compliance becomes operational, embedded directly into transactions rather than enforced through after-the-fact reviews.

The Strategic Value of KoreID Entity

KoreID Entity provides the missing infrastructure layer between fragmented KYB processes and fully governed private markets. It enables:

- Faster onboarding without compromising regulatory rigor
- Reduced counterparty and operational risk
- Clear entity-level accountability and auditability
- Scalable compliance across jurisdictions and entity types

Most importantly, it ensures that when a business participates in a private-market transaction, the entity itself, not just its representatives, is provably authorized, compliant, and trusted.

Know Your Asset (KYA)

Asset-Grade Trust for Regulated Private Markets

Markets do not regulate identities or transactions in isolation. They regulate assets—what exists, what rights it carries, and how it may move.

Know Your Asset (KYA) is the ability to clearly, continuously, and defensibly prove that an asset is precisely defined, legally recognizable, and compliant with applicable regulatory and contractual constraints at any point in its lifecycle.

KYA is the asset-level assurance that regulators, auditors, issuers, platforms, and counterparties ultimately rely on.

The KYA Problem

Traditional financial systems assume the asset is understood:

- Securities are described in offering documents
- Real-world assets are referenced through contracts
- Digital assets are represented by tokens or metadata

But in practice, asset-related failures occur because:

- The asset was ambiguously defined
- Rights and restrictions were unclear or inconsistently enforced
- Regulatory classification changed or was misapplied
- Asset state (at rest vs. in motion) could not be reconstructed
- On-chain or off-chain representations diverged from legal reality

Static descriptions and siloed records do not establish asset legitimacy.

KYA: The Missing Layer

Know Your Asset (KYA) is the asset-level assurance that emerges when legal definition, regulatory classification, economic rights, and technical representation are bound

together into a single, verifiable asset identity.

KYA answers one core question: Is this specific asset what it claims to be, legally, economically, and operationally, and can that be proven over time?

The Foundations of KYA

KYA is established through a governed asset identity framework that persists across the asset lifecycle.

Asset Definition and Classification

KYA establishes and maintains:

- Asset type (security, real-world asset, NFT, digital twin, hybrid)
- Asset class and subtype (equity, debt, fund interest, derivative, utility-linked)
- Jurisdictional and regulatory classification
- Applicable legal frameworks and regimes

This ensures the asset is legally recognizable and correctly categorized.

Rights, Restrictions, and Attributes

KYA captures and governs:

- Economic rights (ownership, dividends, interest, conversion)
- Control rights (voting, governance, redemption)
- Transfer restrictions and lockups
- Jurisdictional, investor, or role-based constraints

This ensures the asset's behavior aligns with its legal and regulatory intent.

Quantity, State, and Provenance

KYA continuously tracks:

- Authorized supply and issuance limits
- Asset state (issued, outstanding, retired, frozen, pledged)
- At-rest vs. in-motion status
- Provenance, lineage, and lifecycle events

This ensures the asset's history and current status are auditable and defensible.

Representation and Binding

KYA binds:

- Legal documentation
- Off-chain records and attestations
- On-chain representations (tokens, hashes, identifiers)
- Oracle-mediated state changes

This ensures technical representations do not drift from legal reality.

What KYA Proves

An asset achieves KYA when the following are provably true:

1. **Definitional Clarity**
   - The asset is uniquely identifiable
   - Its type, class, and structure are unambiguous
2. **Regulatory Validity**
   - Applicable regulations are known and enforced
   - Asset behavior conforms to jurisdictional requirements

3. **Rights and Restrictions Integrity**

- Rights are explicit and enforceable

- Restrictions are consistently applied

4. **State and Lifecycle Accuracy**

- Asset state is current and provable

- Historical states can be reconstructed

5. **Representation Consistency**

- On-chain and off-chain views are synchronized

- Legal, economic, and technical layers remain aligned

6. **Ongoing Validity**

- Changes in regulation, ownership, or risk are monitored

- Assets can be restricted, remediated, or reclassified

- Historical asset states remain defensible over time

Why KYA Matters

- **For regulators:** Clear, asset-level visibility into what exists and how it may behave—not assumptions.

- **For issuers:** Reduced legal ambiguity, fewer post-issuance surprises, and defensible asset structures.

- **For platforms and intermediaries:** Consistent enforcement of asset rules across systems and jurisdictions.

- **For markets:** Trust shifts from fragmented descriptions to provable asset legitimacy.

KYA in the KoreID Trust Model

KoreID Individual verifies people.

KoreID Entity verifies organizations.

KYA verifies assets.

KYT proves transactions.

Together, these layers establish a complete, transaction-grade trust framework spanning who may act, what may be transacted, and how that transaction may occur, designed for auditability, enforceability, and scale.

Know Your Transaction (KYT)

Transaction-Grade Trust for Regulated Private Markets

Markets do not regulate identities in isolation. They regulate transactions.

Know Your Transaction (KYT) is the ability to prove clearly, continuously, and defensibly that a specific transaction between verified parties was authorized, compliant, and enforceable at the moment it occurred. KYT is the outcome that regulators, auditors, platforms, and counterparties ultimately care about.

The KYT Problem

Traditional compliance frameworks focus on onboarding checks:

- KYC verifies individuals
- KYB verifies entities

But compliance failures rarely occur because identity was unknown. They occur because:

- Parties were not eligible at the time of action
- Authority to act was unclear or outdated
- Required disclosures were not properly attested
- Transactions could not be reconstructed or defended later

Static, point-in-time checks do not establish transaction legitimacy.

KYT: The Missing Layer

Know Your Transaction (KYT) is the transaction-level assurance that emerges when verified identities, verified entities, and governed execution are bound together. KYT answers one core question: *Was this specific transaction valid, authorized, and compliant when it happened and can that be proven later?*

The Foundations of KYT

KYT is established through the combination of two persistent identity layers:

KoreID Individual — KYC

Establishes and continuously monitors:

- Verified natural persons
- AML risk, sanctions, suitability, and eligibility
- Role- and action-based authorization
- Verified public wallet ownership
- Consent, approvals, and authentication

KoreID Individual ensures that *a person is who they claim to be and is eligible to act.*

KoreID Entity — KYB

Establishes and continuously monitors:

- Legal existence and good standing of organizations
- Ownership, control, and authority to bind the entity
- Regulatory registrations and licensing scope
- Role-specific permissions (issuer, broker-dealer, ATS, transfer agent, service provider)

KoreID Entity ensures that *an organization is legally authorized to participate and transact.*

What KYT Proves

A transaction achieves KYT when the following are provably true:

1. Verified Parties

- Individuals are KYC-verified
- Entities are KYB-verified
- Regulated intermediaries are authorized
- Applicable regimes are identified (e.g., JOBS Act, jurisdictional rules)

2. Authority and Eligibility

- Each party is authorized to perform *this specific action*
- Authority is valid at the moment of execution
- Role, jurisdiction, and regulatory scope are enforced

3. Disclosures and Attestation

- Required disclosures are delivered
- Attestations are captured and bound to the transaction
- Evidence of acknowledgment is preserved

4. Consent and Acceptance

- eSignatures and approvals are recorded
- Acceptance is unambiguous and attributable
- Timing and sequencing are provable

5. Transaction Integrity

- Transactions are cryptographically hashed

- Execution is timestamped and immutable
- Records are audit-ready and non-repudiable

6. Ongoing Validity

- Post-transaction monitoring detects changes in risk or status
- Revocation, restriction, or remediation can be triggered
- Historical transactions remain defensible over time

Why KYT Matters

- **For regulators:** Clear, transaction-level evidence of compliance, not assumptions.
- **For platforms and issuers:** Reduced risk, fewer enforcement surprises, and faster time to market.
- **For intermediaries:** Defensible audit trails and continuous compliance without manual rework.
- **For markets:** Trust shifts from fragmented checks to provable transaction legitimacy.

KoreID
Inclusivity

The Inclusive Identity
& Compliance Passport
for Global Private
Capital Markets

Executive Summary

The global identity landscape is rapidly fragmenting. Governments are rolling out national digital identity wallets. Blockchain ecosystems are introducing on-chain and zero-knowledge identities. Enterprises rely on commercial identity proofing and KYC/KYB providers.

Each of these identity systems excels within its own domain, but none are designed to operate across jurisdictions, asset types, regulatory regimes, and market structures that define modern private capital markets.

KoreID is not another identity system. It is a market-grade identity orchestration and compliance passport that integrates, normalizes, and extends existing identities, government, blockchain, and commercial into a single, reusable trust layer purpose-built for regulated private markets.

KoreID is inclusive by design. It accepts, augments, and interoperates with other IDs, rather than attempting to replace them.

The Core Problem KoreID Solves

Most identity solutions are built to answer one narrow question:

- *"Who is this person?"*
- *"Is this a unique human?"*
- *"Can this user log in?"*
- *"Did this entity pass KYC once?"*

Private capital markets require far more:

- Continuous verification, not one-time checks
- Entity and individual identity together, including ownership and control

- Jurisdiction-specific eligibility, suitability, and regulatory constraints
- Authorization for specific financial actions, not just authentication
- Binding of verified identities to wallets, transactions, and market events
- Auditability for regulators, intermediaries, and fiduciaries

KoreID exists to unify these requirements while leveraging the best identity signals already available in the market.

KoreID's Inclusive Identity Model

KoreID acts as a trust aggregation and enforcement layer:

- **Ingests** trusted identity signals from external systems
- **Normalizes** them into market-ready identity and compliance claims
- **Continuously monitors** those claims over time
- **Authorizes transactions and actions** based on real-time status
- **Exports attestations** to blockchain, TradFi, and regulatory workflows

This allows KoreID to sit *above* existing identity initiatives, connecting them into a single operational framework for private markets.

Identity Category	What These IDs Do Well	Structural Limitation (Why KoreID Is Needed)
Government Digital IDs & Wallets (e.g., national eIDs)	High-assurance legal identity; government-backed verification; strong authentication	Not designed for capital markets; no AML/sanctions programs, no suitability or eligibility logic, no entity ownership modeling, no transaction authorization

Identity Category	What These IDs Do Well	Structural Limitation (Why KoreID Is Needed)
Blockchain / On-Chain IDs (e.g., wallet-linked or ZK identities)	Cryptographic proof, composability, on-chain enforcement, privacy-preserving attestations	Typically lack legal identity grounding, regulatory accountability, off-chain entity context, and continuous compliance monitoring
Proof-of-Personhood IDs	Human uniqueness, anti-bot and Sybil resistance	Do not establish legal identity, financial eligibility, or regulatory compliance
Commercial KYC / KYB Providers	Efficient onboarding, document verification, sanctions screening	Point-in-time checks; limited portability; no market-wide authorization layer; weak cross-platform reuse
Enterprise Login / IAM Systems	Secure authentication and access control	Identity without regulatory meaning; no compliance, suitability, or transaction context

KoreID incorporates the strengths of each while addressing their limitations.

What Makes KoreID Different

KoreID is purpose-built for regulated private capital markets, where identity must support:

- Individuals, entities, assets, and transactions
- Primary and secondary transactions
- TradFi, blockchain, and hybrid environments
- Retail, accredited, and institutional participants
- Issuers, broker-dealers, transfer agents, platforms, and regulators

Key differentiators:

- **Identity + Compliance + Authorization:** Unification of IDs
- **Continuous monitoring:** Not static approval
- **Entity-aware identity:** Including ownership and authority
- **Wallet-verified identity:** Linked to real economic activity
- **Transaction-level trust (KYT):** Not just participant trust

KoreID as a TradFi/DeFi Briding & Integration Layer

KoreID is designed to work with the existing ecosystems, not replace them:

- Government IDs can serve as high-assurance identity inputs
- Blockchain IDs and credentials can be consumed and validated
- Commercial KYC/KYB providers can be plugged in as verification sources
- KoreID credentials can be issued outward for reuse across platforms

KoreID facilitates seamless workflows that transition between the TradFi and DeFi ecosystems, thus expanding the liquidity reach of DeFi with the trust assurance of TradFi as well as enabling both ecosystems to innovate financial products and services.

ID Category	TradFi	DeFi
Government IDs	Regulatory and Institutional bodies	Unregulated or quasi-regulated decentralized financial networks
Blockchain IDs	Permissioned and compliant blockchain networks	Public blockchain networks and applications with or without compliant ID

ID Category	TradFi	DeFi
Commercial IDs	KYC/KYB providers	On-chain KYC/KYB records with off-chain KYC/KYB
Kore ID	Seamless workflows across TradFi and DeFi	

This architecture allows markets to evolve without fragmentation—while maintaining regulatory integrity.

Strategic Positioning

KoreID is the connective tissue of trust for private markets.

It enables:

- Faster onboarding without sacrificing compliance
- Reduced duplication of identity checks
- Lower regulatory and operational risk
- Seamless interoperability across systems and jurisdictions

Rather than competing with identity initiatives, KoreID makes them usable where it matters most in real, regulated financial transactions.

Summary

KoreID is the inclusive, market-grade identity passport that unifies government IDs, blockchain identities, and commercial verification into a single compliance and transaction authorization layer for global private capital markets.

![Kore Inside logo]

KoreID:
A Comparative Analysis of Digital Identity Systems

A Compliance-First
Meta-Identity for
Capital Markets

Abstract

Digital identity systems have evolved across multiple domains, including government registries, enterprise authentication systems, financial market identifiers, and decentralized identity frameworks. Each of these systems solves a specific problem, but none provides a unified identity infrastructure capable of linking verified participants, regulatory compliance, financial assets, and transaction authorization.

This fragmentation creates significant friction across financial ecosystems. Market participants repeatedly undergo identity verification, regulatory checks, and onboarding processes across different platforms.

KoreID introduces a new category of identity infrastructure designed specifically for regulated financial ecosystems. **KoreID** functions as a **compliance-first meta-identity**, linking individuals, entities, assets, and transactions within a unified identity framework.

This whitepaper compares **KoreID** with existing identity systems across consumer technology, enterprise infrastructure, decentralized identity ecosystems, and financial market registries.

1. Identity Fragmentation in Financial Infrastructure

Every financial transaction depends on several identity components:

- participant identity
- legal authority
- asset ownership
- regulatory eligibility
- transaction authorization

Yet modern financial infrastructure manages these components through **independent systems.**

Component	Typical Identifier
Individual identity	SSN, passport
Corporate identity	EIN, LEI
Securities	ISIN, CUSIP
Application login	OAuth, SAML
Blockchain accounts	Wallet addresses

These systems do not interoperate natively.

As a result, financial platforms repeatedly perform the same processes:

- identity verification
- KYC checks
- AML screening
- investor onboarding
- credential management

This fragmentation increases operational cost, regulatory complexity, and user friction.

2. Categories of Identity Systems

Identity technologies today fall into several broad categories.

1. Government identity identifiers
2. Financial market identifiers

33

3. Enterprise authentication frameworks

4. Consumer platform identities

5. Web3 and decentralized identity frameworks

6. Identity verification networks

Each category solves a narrow problem, but none provides a comprehensive identity infrastructure for regulated financial markets.

3. Government and Registry Identifiers

Government identifiers provide official references for individuals and legal entities.

Identifier	Identifies	Authentication	Authorization	Compliance Integration
SSN	Individual	No	No	No
Passport	Individual	No	No	No
EIN	Legal entity	No	No	No
LEI	Legal entity	No	No	Partial
DUNS	Organization	No	No	No

These identifiers function primarily as **registry references.**

They do not provide authentication, authorization, or transaction-level verification.

4. Financial Asset Identifiers

Financial instruments are identified through standardized registries.

Identifier	Identifies	Authentication	Compliance Integration
ISIN	Securities	No	No
CUSIP	Securities	No	No
SEDOL	Securities	No	No

These identifiers allow markets to identify financial instruments but do not identify transaction participants.

5. Enterprise Authentication Frameworks

Enterprise systems manage application access through authentication protocols.

Standard	Authentication	Authorization	Verified Identity	Compliance Integration
OAuth2	Yes	Partial	No	No
OpenID Connect	Yes	No	No	No
SAML	Yes	Yes	No	No

These frameworks manage login credentials but do not verify real-world identity or regulatory eligibility.

6. Consumer Platform Identity Systems

Large technology platforms operate identity systems for consumer ecosystems.

Identity System	Domain	Authentication	Authorization	Compliance
Apple ID	Apple ecosystem	Yes	Limited	No
Google ID	Google ecosystem	Yes	Limited	No
Microsoft Entra ID	Enterprise ecosystem	Yes	Yes	No

These identities enable convenient login but remain confined to proprietary ecosystems.

7. Decentralized Identity Systems

Blockchain ecosystems have introduced decentralized identity frameworks intended to give users greater control over identity credentials.

System	Identifies	Authentication	Compliance	Governance
DID	Individuals/ entities	Yes	No	Decentralized
Verifiable Credentials	Identity claims	Partial	No	Decentralized
Wallet address	Blockchain account	Yes	No	Protocol

These systems support portable identity credentials but typically assume pseudonymous participation incompatible with regulated financial markets.

8. Digital Identity Networks and Verification Platforms

Several platforms provide reusable identity verification, proof-of-personhood, or digital onboarding services.

Examples include:

Platform	Identity Model	Core Capability
ONCHAINID	Web3 identity	Blockchain-based digital identity
World ID	Proof-of-personhood	Biometric identity verification
eID-Me	Digital identity	Government-grade digital identity
CLEAR	Identity verification	Biometric identity network
GlobaliD	Digital identity network	Portable identity profile
SpruceID	SSI infrastructure	Verifiable credential framework
Trinsic	SSI infrastructure	Identity wallet infrastructure
Privado ID (Polygon ID)	ZK identity	Privacy-preserving identity
Civic	Blockchain identity	Identity verification services
Fractal ID	Web3 identity	Self-sovereign verification

Platform	Identity Model	Core Capability
ID.me	Identity network	Government/enterprise identity verification
Persona	Identity verification	Developer identity APIs
Veriff	Identity verification	AI identity verification
Jumio	Compliance identity	AML/KYC verification
Onfido	Identity verification	Document + biometric identity

These platforms offer identity verification and onboarding services but typically do not integrate identity with financial assets or transactions.

9. Capability Comparison Across Identity Systems

Identity System	Authentication	Authorization	Compliance Integration	Asset Linkage	Transaction Context	Portability
Government IDs	No	No	No	No	No	Limited
Enterprise identity	Yes	Yes	No	No	No	Limited
Consumer platform IDs	Yes	Limited	No	No	No	Limited

Identity System	Authentication	Authorization	Compliance Integration	Asset Linkage	Transaction Context	Portability
Decentralized IDs	Yes	Limited	No	No	No	High
Identity verification networks	Partial	Limited	Partial	No	No	Moderate
Financial identifiers	No	No	No	Yes	No	High
Kore ID	Yes	Yes	Yes	Yes	Yes	High

KoreID uniquely integrates identity verification, authorization, regulatory compliance, asset linkage, and transaction participation.

10. Identity Scope Comparison

System	Person	Entity	Account	Wallet	Asset	Transaction
Apple ID	Yes	No	Yes	No	No	No
Google ID	Yes	No	Yes	No	No	No
Enterprise Identity	Yes	Yes	Yes	No	No	No
DID	Yes	Yes	Partial	Yes	No	No
Wallet Address	Yes	No	Yes	No	No	No

System	Person	Entity	Account	Wallet	Asset	Transaction
Financial Identifiers	No	Yes	No	No	Yes	No
Identity Verification Platforms	Yes	Partial	Partial	No	No	No
Kore ID	Yes	Yes	Yes	Yes	Yes	Yes

11. KoreID as a Meta-Identity Layer

KoreID links identity across multiple layers.

Individual / Legal Entity → Accounts → Wallets → Assets → Transactions

This structure allows **KoreID** to function as a **meta-identity layer across financial infrastructure.**

12. Architectural Model

Traditional systems separate identity, authorization, and compliance.

Traditional workflow

User login → Application authentication → Compliance verification → Transaction processing

KoreID workflow

Verified identity → Authorization policy → Compliance verification → Transaction eligibility → Asset interaction

This architecture embeds compliance directly within identity infrastructure.

13. Where KoreID Sits in the Capital Markets Infrastructure Stack

Financial markets rely on several foundational infrastructure layers.

Infrastructure Layer	Examples
Network infrastructure	Internet, cloud providers
Messaging infrastructure	SWIFT
Trading protocols	FIX
Market data	Exchanges, market feeds
Clearing and settlement	DTCC
Payment rails	Visa, Mastercard
Identity infrastructure	Kore ID

KoreID introduces an identity infrastructure layer that connects participants, assets, and transactions across capital market platforms.

14. Strategic Implications

If widely adopted, **KoreID** could function as a foundational infrastructure layer for capital markets.

Comparable infrastructure roles include:

Infrastructure	Examples
SWIFT	Banking messaging
Visa	Payment authorization
DNS	Internet naming
FIX	Trading communication
Kore ID	Identity and compliance infrastructure

Rather than functioning as a consumer identity system, **KoreID** is designed as an **underlying infrastructure for financial ecosystems.**

15. Conclusion

Digital identity systems today remain fragmented across government registries, enterprise authentication frameworks, decentralized identity ecosystems, and identity verification networks.

These systems identify participants, authenticate users, or verify credentials, but do not integrate identity with asset ownership, regulatory compliance, and transaction authorization.

KoreID introduces a compliance-first meta-identity architecture that unifies these dimensions within a single identity infrastructure.

By linking individuals, entities, assets, and transactions, **KoreID** provides a foundation for interoperable identity infrastructure capable of supporting modern capital markets.