

AI DIGIMARKET LLC

Digital ID for CBDC

Trusted identity. Authorized transactions. Auditable decisions.

Smarter System. Smarter Business.

A digital identity and authorization layer for CBDC ecosystems

SmartDefense Digital ID for CBDC is designed to help central banks, financial institutions, payment operators and approved service providers verify participants, bind trusted identities to wallets or accounts, apply authorization policies, and preserve an auditable record of access and transaction decisions.

Designed as an integration layer - not a replacement for a central bank, national Digital ID, KYC program, wallet platform or CBDC ledger.

Why Digital ID Matters for CBDC

A CBDC can move value digitally, but a trusted transaction ecosystem also needs a way to determine who is participating, what they are authorized to do, which wallet or account belongs to them, and when additional approval is required. SmartDefense Digital ID for CBDC provides the identity-and-authorization layer around those decisions.

Identity Question	SmartDefense Function	Result
Who is this participant?	Verify an approved credential or identity source.	A known identity context for the transaction.
Which wallet/account is theirs?	Bind approved identity context to institutional accounts or wallets.	Reduced ambiguity between person, institution and payment endpoint.
What may they do?	Evaluate role, eligibility, limits, jurisdiction, purpose and approval requirements.	Authorized access and transaction scope.
What happened?	Record the identity, policy, approval, decision and transaction outcome.	Traceable evidence and accountability.

Core design principles

- Identity does not automatically equal authorization.
- Access should be bounded by role, institution, purpose, resource, transaction type and time.
- Least privilege and default-deny policies should protect sensitive functions.
- High-impact actions can require step-up authentication or multi-person approval.
- Identity data should be minimized and separated from unnecessary transaction details wherever practical.
- Every important authorization decision should be traceable to the policy and evidence used at that time.

Central bank authority remains central

SmartDefense can coordinate identity, eligibility, approvals and connected transaction workflows. Issuance, monetary policy, settlement authority and finality remain with the central bank and the connected payment or ledger infrastructure.

How the Digital ID for CBDC Workflow Works

Step	Function	What Happens
1	Enroll / Verify	Validate an approved digital identity, bank/KYC credential or other authorized identity source.
2	Bind	Associate the verified identity context with an approved wallet, account or institutional endpoint.

3	Authenticate	Confirm the participant at the moment of access or transaction using configured authentication methods.
4	Authorize	Evaluate eligibility, transaction limits, role, purpose, jurisdiction, risk conditions and approval requirements.
5	Transact	Route the approved request to the connected CBDC/payment interface or simulator.
6	Record	Preserve the policy version, approvals, transaction status, exceptions and final outcome in the audit record.

Authorization is more than login

A participant may be successfully authenticated and still not be authorized for a specific transaction. SmartDefense can evaluate additional policy context before permitting an action.

Role Retail user, bank operator, merchant, government disbursement officer, treasury user or approved service account.	Institution The bank, payment provider, government agency or other institution under which the identity is acting.
Purpose The reason access or a transaction is being requested.	Resource The wallet, account, asset, function or dataset being accessed.
Transaction Context Amount, type, frequency, jurisdiction, risk flags and other configured rules.	Time & Approval Session age, temporary entitlement, step-up authentication, supervisor approval or dual control.

Technology Capabilities

Capability	Role in the CBDC Identity Layer
Digital Identity Integration	Connect approved identity providers, credentials and institutional identity systems through controlled interfaces.

Authentication	Support configured sign-in and step-up methods appropriate to the deployment environment.
Authorization / Policy Engine	Evaluate role, institution, purpose, resource, transaction rules, eligibility and approval requirements.
Wallet / Account Binding	Associate verified identity context with approved wallet or account relationships.
API & CBDC Adapters	Connect to approved payment, wallet or CBDC interfaces when access and suitable APIs are available.
Cryptographic Integrity	Use digital signatures, hashing and tamper-evident techniques to help protect the integrity of records and evidence.
Audit & Evidence	Record access, authorization decisions, approvals, policy versions, transaction status and exceptions.
AI Assistance	Assist document review, anomaly triage and exception handling while preserving human authority for consequential decisions.
Monitoring & Incident Response	Track access anomalies, failed authorization, service health and security events with escalation workflows.
Privacy & Data Governance	Support data minimization, retention rules, separation of duties and jurisdiction-specific governance requirements.

Security model

- Authentication is required, but it is never treated as unlimited authorization.
- Policy checks are enforced server-side and at integration boundaries, not only in the user interface.
- Privileged administrative access can be separated from normal transaction authority.
- Temporary or emergency permissions should expire automatically and remain auditable.
- Sensitive actions can require maker-checker or multi-person approval.
- Secrets, keys and service credentials should be protected by dedicated key/secret-management controls.
- Finance and Command environments can reuse common technology without inheriting each other's data permissions.

Example CBDC Use Cases

Use Case	SmartDefense Digital ID Role
Retail Wallet Enrollment	Verify a participant through an approved identity source and bind that identity context to a CBDC wallet.

Merchant Access	Verify a business or authorized representative and control permitted payment and settlement functions.
Government Disbursement	Authorize defined government users and recipient identities for benefit, grant or emergency-payment workflows.
Institutional / Wholesale Access	Control treasury, bank or approved institutional access using role and transaction policies.
Transaction Exception Review	Route high-value, unusual or policy-exception transactions to an authorized reviewer.
Cross-System Reconciliation	Track identity, approval, payment and ledger events without assuming atomic finality across separate systems.

A practical pilot path

1. Select one CBDC or payment use case and one participant type.
2. Connect one approved identity source and one wallet/account model.
3. Define authorization policy, transaction limits and approval paths.
4. Integrate with a CBDC sandbox, simulator or approved payment interface.
5. Test enrollment, authentication, wallet binding, authorization, exceptions and revocation.
6. Measure onboarding time, blocked access, manual exceptions, audit completeness and recovery behavior.
7. Expand only after governance, security and operational controls are validated.

Product positioning

SmartDefense Digital ID for CBDC is an identity, authorization and transaction-workflow layer. It is intended to interoperate with approved national Digital ID, banking, payment and CBDC infrastructure - not replace them.

Proposed capabilities and development roadmap. Integration scope, legal requirements, privacy controls and production access depend on the applicable jurisdiction and participating institutions.