CONFIDENTIAL

TECHNOLOGY OVERVIEW

How iDen2 works

A cryptographic identity platform that issues, verifies, and federates credentials for humans, organizations, AI agents, and devices, on open standards, deployable anywhere.

KYC Know your customer

KYA Know your agent

KYD Know your device

KYB Know your business

Verify once. Trust everywhere.

Alfy Louis
Founder & CEO

IN ONE SLIDE

One platform, four kinds of identity

Most identity systems assume the subject is a person logging into an application. iDen2 treats identity as a cryptographic primitive that applies equally to people, organizations, machines, and the AI agents now acting on their behalf.

People

Citizens and customers holding their own credentials, disclosing only what each situation requires.

Organizations

Companies and agencies that issue, verify, and carry credentials of their own, including legal-entity identity.

AI agents

Software actors carrying a scoped, revocable mandate traceable to an accountable human or organization.

Devices

Vehicles, sensors, and IoT presenting identity and payment-bound credentials autonomously.

The same issuance, verification, and revocation machinery serves all four. There is no separate system for agents.

ARCHITECTURE

Five layers, interface to data

Five independently deployable layers. That separability is what makes on-premise, hybrid, and air-gapped installations practical.

Layer 01 · Interface How entities access the platform	Holdr Wallet (iOS · Android · Web) · Enterprise admin console · Developer portal & sandbox · Government dashboard · white-label apps
Layer 02 · API Gateway Programmatic access surface	REST API v2 · GraphQL · CAMARA / GSMA Open Gateway · Webhook event bus · SDKs for iOS, Android, Node, Python, Java, Go
Layer 03 · Core Identity Engine Cryptographic credential operations	VC issuance (W3C VC 2.0) · protocol translation across 7 formats · ZK proof generator · APoC engine · DID resolver and registry
Layer 04 · Security & Trust Cryptographic primitives and biometrics	ISO 30107-3 PAD L3 liveness · post-quantum ML-DSA and ML-KEM · SIM-bound biometric anchor · HSM key management
Layer 05 · Data & Integration Persistence, federation, external systems	DPKI / DID registry · BSS-OSS connectors · eIDAS node bridge · ICAO trust network (40+ countries) · audit and compliance store

PLATFORM MODULES

Six modules, one identity fabric

The functional breakdown of the core engine. Each module is separately addressable through the API, so customers adopt what they need rather than the whole platform at once.

01 Credential Factory

W3C VC 2.0 · eIDAS · lossless protocol translation

02 Custody (Holder) Wallet

Consent, delegation and revocation in one place. Hosts policy-governed agents.
iOS · Android · Web · white-label SDK for credential holders

03 Trust Mesh (Engine)

Checks that credentials are real, current and policy-compliant, in real time.
Federation · DID registry · DPKI · cross-org roaming trust

04 APoC Engine

Agentic Proof of Control, identity and authorization for AI agents

05 Biometric Security

ISO 30107-3 PAD L3 liveness · post-quantum cryptography

06 Protocol Bridge

Verifies & Connects to Okta, Azure AD, Salesforce, and all 7 major credential formats.
REST · Graph QL · CAMARA · webhooks · 6-language SDKs

MODULE 01 · CREDENTIAL ENGINE

Seven formats in, any format out

Most platforms pick one credential format and force the ecosystem to match. iDen2 issues all seven natively and is extending lossless translation across every pair, so a credential issued once is accepted everywhere.

W3C VC 2.0

The core issuance format, JSON-LD and JWT-VC

SD-JWT VC

Selective disclosure, minimal PII per presentation

mDL · ISO 18013-5

Device-bound, offline over BLE and NFC

eIDAS ARF · QEAA

EU Digital Identity Wallet, regulated use cases

AnonCreds

Zero-knowledge predicates without revealing data

ICAO DTC

Digital Travel Credential, 40+ country network

X.509 / PKI

Enterprise legacy, TLS, S/MIME, code signing

7 → 1

One API call. No re-issuance.

< 50ms

Translation latency, p99 target

Lossless

No semantic data loss

Stateless

Nothing stored in transit

Native issuance across all seven formats is live today. Full lossless translation across every format pair reaches GA on the v2 roadmap, see slide 12.

MODULE 02 · HOLDR WALLET

Keys that never leave the device

The holder side of the system. One encrypted wallet for every credential format, with private keys bound to the device secure element, iDen2 itself cannot read stored credentials.

Multi-format storage

All formats in one encrypted wallet, with automatic conversion at presentation time.

Biometric-bound encryption

Keys live in the secure enclave or TEE and are non-exportable, even with root access.

Offline presentation

Bluetooth LE (ISO 18013-5) and NFC, built for transit, borders, and low-connectivity sites.

Selective disclosure UI

The holder sees exactly which fields are requested before confirming; ZK proofs cover predicates.

SDK PLATFORMS

- iOS · Swift
- Android · Kotlin
- React Native
- Node.js
- Python
- Go

White-label: full brand control, standalone App Store and Play publishing, custom schemas.

MODULE 03 · TRUST MESH

Federated trust, no central authority

Every issuer, holder, and verifier is a W3C DID anchored to a verifiable key document. A machine-readable governance framework defines who may issue what, to whom, and under what conditions.

CI

Certified Issuer

Government or regulated. eIDAS QEAA or equivalent, highest assurance.

TI

Trusted Issuer

Enterprise, onboarded via registry review. mDL, employee, B2B.

RI

Registered Issuer

Self-registered via API. Internal and developer issuance.

VO

Verifier-Only

Verifies but cannot issue. Retail, healthcare, border control.

SUPPORTED DID METHODS

did:web · did:key · did:jwk · did:iden2 · did:ebsi · did:ion | aligned to eIDAS QEAA, GLEIF vLEI, ICAO

MODULE 04 · APOC ENGINE

IN BETA

Verifiable identity and control for AI agents

The part of the platform no competitor has. No existing standard gives an AI agent a verifiable identity, names who authorized it, bounds what it may do, or records what it did. APoC is that attribution chain.

APoC CREDENTIAL, FIELDS

agentDID	DID of the agent, unique and revocable
principalDID	DID of the human or org that authorized it
capabilityScope	Permitted actions in plain language plus policy
delegationChain	Full chain when an agent delegates to sub-agents
actionLog	Append-only signed log of every action taken
revocationEndpoint	Real-time check, sub-second invalidation

CAPABILITY SCOPE LANGUAGE

```
ALLOW issuePurchaseOrder WHERE amount < $50,000
ALLOW routeShipment WHERE carrier IN approved_list
DENY  modifyContract
DELEGATE TO sub_agent WHERE scope SUBSET_OF this
```

- **Scope narrows at every hop**
  A sub-agent can never exceed its parent's permissions.
- **Sub-second revocation**
  Checked on every action; a compromised agent halts immediately.
- **Regulator-ready**
  Meets EU AI Act Art. 13 and DORA Art. 30 attribution demands.

MODULE 05 · SECURITY & CRYPTOGRAPHY

Certified biometrics, quantum-ready cryptography

The highest commercial liveness certification, post-quantum signatures already deployed, and issuer keys that never leave a certified HSM.

PRESENTATION ATTACK DETECTION

ISO 30107-3 PAD Level 3

Rejects 3D masks, silicone models, and deepfake video in real time. Multi-modal defence retrained every 30 days.

<0.001%
False acceptance

<0.5%
False rejection

ML-DSA

CRYSTALS-Dilithium post-quantum signatures for all signing.

ML-KEM

CRYSTALS-Kyber key encapsulation, hybrid classical mode.

BBS+ / ZK

Multi-message signatures for selective disclosure.

HSM

Issuer keys in FIPS 140-3 L3 HSMs, never leaving the boundary.

An 18-month lead on post-quantum deployment: credentials issued today stay secure for their full validity period.

BUILT TO MEET

- eIDAS 2.0
- SOC 2 Type II
- ISO 27001
- FedRAMP Moderate
- GDPR
- HIPAA
- EU AI Act
- DORA

Architected and engineered to meet these frameworks. Current certification and audit status by framework is available on request.

MODULE 06 · API & SDK

AVAILABLE TODAY

What you can call today

Two services are live: Issuer as a Service and Verification as a Service, over OID4VCI and OpenID4VP with SD-JWT selective disclosure. RESTful, OpenAPI 3.1, HTTP Basic Auth.

CORE API ENDPOINTS

POST	`/api/v1/issuer/offers`	Create an OID4VCI credential offer	●
GET	`/api/v1/issuer/offers/{id}`	Poll issuance status	●
POST	`/api/v1/verifier/sessions`	Open an OpenID4VP verification	●
GET	`/api/v1/verifier/sessions/{id}`	Retrieve disclosed claims	●
POST	`/v2/credentials/translate`	Format to format, lossless	●
POST	`/v2/apoc/register`	Register an AI agent	●
POST	`/v2/apoc/verify-action`	Allow or deny an agent action	●

RATE LIMITS & TARGETS

100k
req/min · design capacity

45ms
p50 latency

120ms
p99 latency

99.999%
availability target

Developer portal & sandbox

Interactive OpenAPI 3.1 explorer, synthetic test credentials, mock verifiers, and pre-configured DID pairs. Signed HMAC webhooks for issued, presented, revoked, and expired events.

Green = live on staging (v1.0.0, April 2026). Amber = on the v2 roadmap. Latency and availability figures are design targets measured on staging, not contracted SLAs.

DEPLOYMENT

Three modes, one codebase

The same platform, whether it runs in our cloud or inside an air-gapped facility you control. This is what makes sovereign and regulated deployments possible.

Managed cloud

Live in days

- Multi-region AWS, GCP, or Azure, active-active across 3 regions
- Automated failover under 30s RTO
- Daily encrypted backups, 30-day retention
- SOC 2 Type II and ISO 27001 certified datacentres

On-premise / private

90-day SLA

- Containerised Helm deployment for Kubernetes
- Air-gapped option for classified environments
- FIPS 140-3 L3 HSM, Thales, Entrust, CloudHSM
- Customer-controlled keys (BYOK)

Hybrid

Split-plane

- Credential engine on-prem, Trust Mesh in cloud
- Biometric processing local, templates never leave
- Data plane on-prem, control plane SaaS
- Compliance boundaries for GDPR, HIPAA, classified

45ms	120ms	180ms	< 1s	99.999%	< 50ms
API p50	API p99	Issuance p50	Revocation	Uptime target	Translation

STRAIGHT ANSWER

Shipping today versus on the roadmap

The honest line. Everything on the left is in production or on staging now; the right is where the platform is going, with foundations already in code.

AVAILABLE TODAY

- Issuance and verification APIs, OID4VCI, OpenID4VP
- SD-JWT selective disclosure and zero-knowledge proofs
- Holder Wallet, iOS, Android, Web, white-label SDK
- Core formats, W3C VC 2.0, SD-JWT, mDL, ICAO DTC
- ISO 30107-3 PAD L3 biometrics, post-quantum signing
- Trust Mesh, DID methods, developer sandbox
- Deployment in all three modes, incl. air-gapped

ON THE ROADMAP

- APoC Engine, agent registration, scope, action verification
- Agent-to-agent delegation chains at production scale
- Full 7-format lossless translation at GA
- Wallet automation, policy engine and credential lifecycle
- Credential marketplace and interoperability hub
- Liability framework for agent-initiated actions

THE TRUST LAYER FOR THE AGENTIC ERA

Know who's acting.
Know what they can do.

Issue, verify, and federate credentials for humans, organizations, AI agents, and devices, on one cryptographic identity platform.

WEBSITE

iden2.com

EMAIL

info@iden2.com

DOCS

docs.iden2.com