CONFIDENTIAL

ONE iDENTITY WALLET

Human identity and agentic identity, bound in one chain of trust.

We bind who you are to what your AI agents may do.

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 Depth

Company communication deck · July 2026

THE BIG PICTURE

The ecosystem at a glance

TRUSTED ISSUERS

Telecom
- Verifies identity
- Manages SIM & device
- Communication channel

Bank
- Verifies identity
- Income & address
- Ongoing monitoring

Government
- Issues official IDs
- Verifies citizens

Employer
- Verifies employment status

They verify facts about you.

USER WALLET

Verified identity
by Telecom ✓

KYC credential
by Bank ✓

Age credential
by Government ✓

Employment credential
by Employer ✓

Owned by you. Portable. Private.

AI agents

RELYING PARTIES

- E-commerce
- Insurance
- Fintech
- Travel
- Healthcare
- Education
- Enterprise apps
- Mobility

They accept credentials with your consent.

THE PLATFORM

A modular trust operating system: Phenix®.

PHENIX

No rip and replace required, five modules, one root of trust.

ISSUANCE · PHENIX®

Credentials Factory

Creates verifiable digital IDs from any identity source, with a full audit trail.

VERIFICATION

Trust Engine

Checks that credentials are real, current and policy-compliant, in real time.

INTELLIGENT WALLETS

Custody Control

Consent, delegation and revocation in one place. Hosts 5 policy-governed agents.

AI CONTROL

CAPoC Engine

Proves an AI agent is authorized. Every action signed by a real person.

INTEGRATION

Verification Gateway

Connects to Okta, Azure AD, Salesforce, and all 7 major credential formats.

Standards-aligned · W3C VC 2.0 · eIDAS 2.0 · ISO 18013-5 · NIST SP 800-63 · ML-DSA / FIPS 204 (post-quantum)

WHY NOW

AI agents started acting. Identity broke in a new way.

An AI agent books your flight, files your claim, pays your vendor. The party on the other side faces a question the internet has never had to answer before, and OAuth tokens, API keys, and passwords were never built to answer it.

1

Who authorized this agent?

Is there a real, identifiable human behind it, or a script wearing a stolen key?

2

Are they still in control?

They authorized it last month. Have they forgotten it? Lost the device? Are they even alive?

3

Is it still the same agent?

Or have its instructions and tools been quietly rewritten since the day it was approved?

By 2027, Gartner expects 40% of enterprises to decommission or demote autonomous AI agents over governance gaps found only after a production incident. Incumbents credential the agent, not the verified human behind it.

THE GAP

Everyone picked one side. The trust question lives in the middle.

Identity verification vendors

Verify the human, then stop.

KYC, document checks, biometrics. The moment a verified person hands work to an AI agent, their assurance ends. The agent is invisible to them.

Agent-identity protocols

Credential the agent, treat the human as metadata.

Agent DIDs, delegation records, agent-to-agent handshakes. Useful plumbing, but nobody proves which verified human stands behind the agent right now.

eIDAS / government wallets

Hold human credentials, no agent story.

eIDAS 2.0 obliges every member state to offer a wallet by December 2026. Not one of them answers what happens when the citizen delegates to AI.

iDen2 lives in the middle: verified human identity and agentic identity bound in one wallet, under continuous proof.

iDen2 binds your verified real-world identity and your AI agents' credentials in one iDentity Wallet,

So every action an agent takes traces, cryptographically and continuously, to a real human who is provably still in control.

One wallet. One unbroken chain of trust. Verifiable by anyone, even offline.

WHAT “BOUND” MEANS

Two kinds of credentials that never lived together before

YOUR HUMAN IDENTITY

Issued by parties the world already trusts

- ✓ Government ID & eIDAS attributes
- ✓ KYC verification from your bank
- ✓ Professional licenses & employment
- ✓ Health coverage, age, loyalty status

Held in your wallet, selectively disclosable. iDen2 never sees the attributes.

+

YOUR AGENTS’ IDENTITY

Issued under your authority

- ✓ A DID for every agent that acts for you
- ✓ Delegation: scope, limits, time bounds
- ✓ The exact configuration you approved
- ✓ Live proof your control is still alive

Rooted in your verified identity, not a free-standing API key.

The binding is cryptographic and continuous; an agent’s credential stays alive only while your control stays alive.

HOW THE BINDING WORKS

Five steps, no new trust required

1	**Your verified identity enters the wallet**	Banks, IDV providers, and government issuers place verifiable credentials in your iDentity Wallet. Issuers verify; iDen2 binds.
2	**You create an agent under your identity**	The wallet issues the agent a delegation credential rooted in your identity: scope, limits, counterparties, time bounds, signed by you.
3	**The binding stays alive, not archived**	Your wallet releases signed, timestamped heartbeat envelopes. The agent’s authority is valid only while evidence of your control is fresh.
4	**Every action carries the whole chain**	Verified human root, delegation, live control, agent integrity, one composite proof, under minimum disclosure, verifiable offline.
5	**Ending it costs nothing**	Go silent and authority decays within the policy window. Publish the kill value and it dies instantly, everywhere it is seen.

THE ENFORCEMENT ENGINE · PATENT PENDING

Continuous Agentic Proof of Control (CAPoC)

The binding is not a database row. It is a living cryptographic condition, three proofs that must all be present, together, at the moment the agent acts.

PROOF 1

Human-rooted delegation

An unbroken chain of signed delegation credentials from a verified human to every agent and sub-agent. Broken anywhere = dead everywhere below.

PROOF 2

Control freshness

A signed, timestamped heartbeat from your wallet keeps authority alive. Silence is the revocation mechanism; authority expires by itself within the policy window.

PROOF 3

Agent integrity

Before any credential is released, the agent must prove its configuration, instructions, tools, model, still matches what you signed. Tampering fails the gate.

High-risk actions escalate automatically: a presence-gated approval on your device, bound to that exact transaction and no other.

THE VERIFIER’S VIEW

Verified offline by the relying party, in milliseconds

A merchant terminal, a claims system, a government portal, any relying party checks the whole chain locally, using nothing but the presentation in front of it.

Delegation chain	Signatures walk back to a verified human root	✓ VALID
Control freshness	Heartbeat age 3.2s ≤ required window 15s	✓ FRESH
Agent integrity	Attestation matches the signed configuration	✓ MATCH
Scope	Action within delegated limits	✓ IN SCOPE

0
verifier network calls

Minimum disclosure throughout: the verifier learns “a verified adult stands behind this agent and is in control”, not who you are.

REVOCATION, REINVENTED

Two ways authority ends. One works with no network at all.

THE QUIET WAY

Silence

Lose the phone. Walk away. Forget the agent exists. Nobody files a ticket and nobody calls a help desk, the heartbeat stops, and the agent’s authority decays to nothing within the policy window. The dead-man’s switch is the default state of the system.

Worst-case latency for an offline verifier = the freshness window. A policy knob, not a promise.

THE LOUD WAY

The kill value

One published value, checked with a single hash, renders the delegation permanently invalid at every verifier that has received it. Employee offboarding, compromised agent, change of heart: one action kills every branch of the agent’s authority tree.

No CRL fetch at verification time. The value propagates once, then every verifier checks it locally with a single hash.

Your identity credentials stay untouched either way, only the agent’s branch is cut.

STRAIGHT ANSWERS

What this does, and what it honestly doesn’t

We bind verified credentials from issuers you already trust.	iDen2 does not verify identity itself, banks, IDV partners, and eIDAS issuers do. We make their assurance extend to agents.
The heartbeat proves the control channel is alive.	Presence-gating (biometric approval) upgrades it to proof the human acted. High-risk actions demand exactly that.
Configuration tampering is caught at the gate.	Content-borne prompt manipulation that leaves configuration intact is contained by scope limits, policy, and intent escalation, structurally contained, not “solved.”
Revocation is instant where the kill value is seen.	For offline verifiers, the bound is the freshness window your policy sets. We tell you the knob instead of hiding it.

We put these on a slide because our buyers’ security teams will find them anyway. Trust is the product.

Eight ways this shows up in the world

Payments · Banking · Healthcare · Insurance · Travel · Higher education · Enterprise · Government

SCENARIO 1 · PAYMENTS

Agentic checkout at the point of sale

A shopper’s agent orders $340 of catering through a cloud POS terminal. The merchant has never seen this agent before and never will again.

WHO BUYS THIS

Merchant acquirers · POS platforms · PSPs

WHAT THE BINDING DOES

The agent presents one composite proof: a KYC-verified cardholder at the root, delegation covering retail purchases to $500, control heartbeat seconds old, configuration matching what the cardholder signed. The terminal verifies offline, in milliseconds.

WHY THEY PAY

Agent-not-present is the next card-not-present fraud wave. Acquirers get a cryptographic accept/decline signal instead of a probabilistic one, and chargeback liability becomes assignable.

SCENARIO 2 · BANKING

The agent that can move real money

THE SITUATION

A customer’s AI agent rebalances her portfolio and pays bills. One day it requests a $25,000 wire to a new payee.

WHO BUYS THIS

Retail banks · wealth platforms · brokerages

WHAT THE BINDING DOES

Routine actions ride the standing binding. The wire crosses the risk threshold, so her wallet escalates: Face ID approval producing an intent-bound envelope valid for exactly that wire and nothing else. A stolen copy is useless for any other transfer.

WHY THEY PAY

Agentic banking without widening the fraud surface, and an audit trail that maps every agent action to a verified customer, a signed scope, and a moment of proven control.

SCENARIO 3 · HEALTHCARE

The caregiver’s agent

THE SITUATION

An adult daughter manages her father’s care. Her agent books specialists, refills prescriptions, and fetches lab results across three provider portals.

WHO BUYS THIS

Health systems · payers · patient-access platforms

WHAT THE BINDING DOES

Her verified identity plus a caregiver authorization credential root the agent. Each portal sees only: an authorized caregiver’s agent, scoped to this patient, control fresh, configuration intact. When her authorization ends, the binding dies with it.

WHY THEY PAY

HIPAA-grade accountability for the fastest-growing access pattern in healthcare, and an answer better than families sharing the patient’s password.

SCENARIO 4 · INSURANCE

First notice of loss, filed by an agent

THE SITUATION

After a fender-bender, the policyholder tells his agent to handle it: FNOL, photos, adjuster scheduling, the rental negotiation.

WHO BUYS THIS

P&C carriers · claims platforms · MGAs

WHAT THE BINDING DOES

The claim arrives rooted in the verified policyholder, identity credential, policy credential, delegation scoped to this claim, live control proof. The delegation’s time bound ends the agent’s access when the claim closes.

WHY THEY PAY

Agent-filed claims arrive with KYC-grade provenance and a signed audit chain, fraud screening gets stronger, not weaker, as automation grows.

SCENARIO 5 · TRAVEL & HOSPITALITY

The agent that rebooks at 2 a.m.

THE SITUATION

A traveler’s agent books a multi-leg trip, and rebooks everything when a flight cancels overnight.

WHO BUYS THIS

Airlines · hotel groups · OTAs · loyalty programs

WHAT THE BINDING DOES

Loyalty status, age, and visa-eligibility attributes flow from the traveler’s wallet under selective disclosure, with the live binding proving authorization and present control. The over-limit upgrade wakes the traveler for an intent-bound approval.

WHY THEY PAY

Airlines and OTAs stop fighting an arms race against bots and start running a credential check: friendly automation carries a verified human root; hostile automation cannot.

SCENARIO 6 · HIGHER EDUCATION

The student’s agent, application to graduation

THE SITUATION

An international applicant’s agent assembles transcripts, submits applications, schedules visa appointments, then handles registration every term.

WHAT THE BINDING DOES

The applicant’s verified identity and academic credentials root the agent. Admissions sees agent-submitted applications with provable human provenance; registration stays inside term-bounded, scope-limited delegations.

WHO BUYS THIS

Universities · ed-tech platforms · credential evaluators

WHY THEY PAY

AI is flooding the admissions funnel. Provenance at the point of submission is cheaper than forensics after, and enrollment verification comes free.

SCENARIO 7 · ENTERPRISE

A workforce of employee agents

THE SITUATION

Every analyst gets an AI agent drafting contracts, querying customer data, filing tickets across dozens of SaaS systems.

WHO BUYS THIS

CISOs · IAM teams · any enterprise deploying agents

WHAT THE BINDING DOES

Each agent is rooted in an HR-verified employee credential; scope mirrors entitlements; every action lands in the audit trail attributed to a person. The day the employee leaves, one revocation kills every agent branch instantly.

WHY THEY PAY

Non-human identity is the fastest-growing gap in enterprise IAM. Binding agents to employees turns thousands of ungoverned service identities into one governable tree per person.

SCENARIO 8 · GOVERNMENT / EIDAS 2.0

The citizen’s agent

THE SITUATION

A small-business owner tells her agent to renew a license, file a VAT declaration, and answer a municipal notice.

WHO BUYS THIS

Member-state wallet programs · GovTech integrators

WHAT THE BINDING DOES

Her eIDAS-verified identity roots the agent’s authority. Each portal receives a presentation satisfying wallet-based authentication while disclosing only what the filing requires, with GDPR-conscious handling of control metadata.

eIDAS 2.0 obliges every member state to offer a wallet by December 2026. Nobody has answered what happens when citizens delegate to AI. Whoever answers it becomes the reference architecture.

MESSAGE ARCHITECTURE

Three pillars carry every conversation

One wallet

Human credentials and agent credentials live and work together in the iDentity Wallet.

W3C VC/DID + SD-JWT · agent DIDs under the holder’s root · one recovery, one audit trail · eIDAS 2.0-aligned

One chain of trust

Every agent action traces to a verified human, at KYC grade, not username grade.

Delegations rooted in issuer-verified identity · composite proof verifiable offline · signed audit record per action

Alive, not archived

The binding is proven continuously, not checked once at setup.

CAPoC (patent pending) · heartbeat envelopes · integrity attestation · risk-adaptive freshness · self-expiry + kill

DEFENSIBILITY

Open standards outside. Proprietary, patent-pending engine inside.

BUILT ON WHAT THE WORLD AGREED ON

- ✓ W3C Verifiable Credentials & DIDs
- ✓ SD-JWT selective disclosure
- ✓ OpenID4VCI · OpenID4VP · DIDComm v2 · ToIP stack
- ✓ eIDAS 2.0 architecture alignment
- ✓ MCP-native identity tools for LLM agents

Lock-in is the enemy of adoption. Standards are the doorway.

OURS, AND HARD TO FOLLOW

- ▸ CAPoC binding engine, patent pending
- ▸ The Intelligent Wallet runtime and policy engine
- ▸ Risk-adaptive freshness: authority tightens as risk rises
- ▸ Developer experience: first credential in under 5 minutes
- ▸ No tracked SSI competitor binds human + agent identity

Competitors would need to rebuild their platform to replicate the binding.

BUSINESS MODEL

Revenue scales with the number of bindings

Base platform licensing plus a dedicated Agentic AI Tier priced per agent DID and operations, every new agent a customer deploys is a new binding under management.

$1.00

Per Wallet Per Month

Developer-first platform launch

$0.15

Per Credential Per Month

Agentic AI Tier live: $400K

$0.03+

Per Credential Verification

Agentic AI Tier: $2.5M · 40–60% premium pricing

Why the tier holds its premium: the binding is architectural. It cannot be bolted onto a passive credential store, which is what every tracked competitor ships today.

Targets from the iDen2 2025–2027 roadmap (May 2026 revision).

DELIVERY

The binding deepens in three phases

PHASE 1 · NOW

Reactive intelligence

Human credentials + agent DIDs in one wallet · automatic minimum disclosure · anomaly flagging on every presentation · AI-ready hooks in the core

PHASE 2

Proactive intelligence

Agent Identity Framework: scoped authority per agent · lifecycle monitoring and instant revocation · enterprise agent dashboard · heartbeat + attestation GA

PHASE 3

Agentic intelligence

Full multi-agent delegation chains · MCP-native identity tools callable from any LLM · pre-credentialed agent registry · cross-enterprise coordination with dual audit

Agentic identity is not a Phase 3 feature. It is a design constraint on every API and data model from day one.

SEE IT, DON’T TAKE OUR WORD

What we can put in front of you today

1 Live animated demo

The full CAPoC mechanism running in a browser: real SHA-256 hash chain, signed heartbeat envelopes, attack scenarios failing in real time, including a self-running 90-second story mode.

2 Working platform

Developer-first APIs: issue a verifiable credential within five minutes of reading the docs. Auto-generated SDKs in 10+ languages.

3 Patent position

CAPoC invention disclosure complete (Rev. 2); provisional application filed. Freedom-to-operate review of the crowded static-delegation space already done.

4 Vertical solutions

Full solution decks for insurance, healthcare, travel & hospitality, and higher education, each mapping the binding to line-of-business use cases.

WHERE YOU COME IN

Three ways to work with us

PARTNERS & PLATFORMS

Design-partner pilots

Bring one agent-facing flow, checkout, claims intake, portal access. We stand up the binding around it in weeks and share the results publicly or privately, your call.

ENTERPRISES

First-mover deployments

Pick the vertical scenario that matches your book of business. Phase 1 delivers human + agent credentials in one wallet with your existing issuers of record.

ISSUERS & TRUST PROVIDERS

New value from KYC you already did

Your existing verification becomes the root of trust for every agent your customers deploy. iDen2 never verifies identity itself, we make your assurance extend to agents.

The agent economy runs on trust that can prove itself.

One iDentity Wallet. One unbroken chain from verified human to every agent action. Alive, minute by minute. Verifiable by anyone, even offline.

Alfy Louis · Founder & CEO · alfy@iden2.com · iden2.com