EXECUTIVE BRIEFING

Trust for the agentic era

Software is starting to act for people. Your customers, staff and partners will soon ask one question: who authorised this, and what is it allowed to 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

iDen2

THE STORY IN ONE SLIDE

Five points to take away

1

The challenge

Trust still relies on documents, passwords and phone calls. They are slow to check and easy to fake.

2

The shift

AI agents are moving from answering questions to acting and paying. Each action needs a person behind it.

3

The opportunity

Rules, fraud pressure and agent adoption are arriving together. Early movers set the terms.

4

iDen2

One wallet binds who a person is to what their agents may do. Open standards, no rip and replace.

5

The proposal

A scoped pilot on one workflow: 1 to 2 weeks of discovery, then 6 to 10 weeks to prove value.

Everything in this deck is a proposal to discuss. Targets and scope are agreed together, from your own baseline.

Four problems you already recognise

01

The same proof, again and again

Customers, staff and partners resend the same documents to every organisation. Each one collects, checks and stores them separately.

02

Weak checks, big risks

Passwords, one-time codes and security questions guard accounts, payments and records. Attackers and breached data beat them.

03

Evidence nobody can trust

Scans and PDFs are easy to copy or alter. Checking one means calling the issuer, which is slow and costly.

04

Agents with no proof of authority

Software now acts inside your systems and on your customers' behalf. Often it runs on a shared account with no named human behind it.

The result is cost, delay and risk spread across onboarding, service, security and audit.

Why today’s controls are running out of road

Control we rely on	Built for	Where it strains
Passwords and one-time codes	A person at a keyboard	Phished, reused and intercepted. Resets add cost.
Security questions and call-centre checks	A person on the phone	Answers sit in breached data. Voice and faces can now be imitated.
Document copies and manual review	Paper and PDFs	Slow, repeated, and hard to prove genuine.
Shared service accounts and API keys	Trusted internal software	No named owner, no scope, no expiry. Hard to audit.
Separate identity systems per organisation	One organisation’s own users	Nothing carries across partners, borders or agents.

These controls still matter. The gap is evidence that travels, and proof of who stands behind an agent.

AI is moving from answering to acting

1 Answer

Chat assistants explain, summarise and draft. A human does the rest.

2 Use tools

Agents read systems, fill forms and call services on a person's behalf.

3 Act and pay

Agents place orders, change records and spend money within set limits.

The industry is already building for this. Card networks have announced ways for merchants to recognise approved shopping agents and see what they may do (Visa Trusted Agent Protocol, Mastercard Agent Pay). Open tool standards such as MCP let agents call business systems. What is still open is simple: who proves the human behind the agent, and for how long?

Pace of adoption will differ by sector and region. The direction is clear; the timing is not.

Four questions every agent must be able to answer

1

Who is it?

Can your system tell this agent from a person, a bot or another agent?

2

Who sent it?

Is there proof that a real, verified person or company authorised it?

3

What may it do?

Is the action within limits, and has the permission expired or been withdrawn?

4

Can you prove it later?

Do you keep evidence of the permission, the decision and the action, for audit and disputes?

Today most businesses can answer one or two of these, for people. Almost none can answer all four, for agents.

Digital identity wallets are becoming public infrastructure

December 2026

Every EU member state must offer citizens at least one certified EU Digital Identity Wallet under eIDAS 2.0.

Around December 2027

Private firms that must use strong customer identification are expected to accept the wallet. Reporting names banking, telecoms, energy, transport and healthcare.

What it means for you

Citizens will hold verified credentials in a wallet and expect to use them. Organisations will need to issue, accept and check them.

Handle with care. Readiness differs by country and some states may miss the first date. Exact duties depend on the regulation text and national rules. Confirm with your counsel. Other regions run their own wallet and digital-ID programmes.

Three waves are meeting at the same time

01

Rules

Wallet and digital-ID programmes are moving from pilots to law. Acceptance duties are coming for regulated sectors.

02

Agents

Customers and staff will bring agents to your front door. Payment networks and platforms are already preparing to receive them.

03

Pressure

Impersonation and account takeover keep getting cheaper to attempt. Old checks add friction without adding much proof.

If you wait. You retrofit under deadline, choose from what others have already settled, and handle agents as exceptions.

If you move now. You prove value on one workflow, help set sector rules, and have a tested foundation when the deadline and the agents arrive.

Where it shows up in your business

Onboarding once, reuse often

Customers, staff and partners prove who they are one time. Every later check starts from a trusted credential.

Safer sign-in and approvals

Wallet approval for sensitive changes, payments and recovery. No code to phish.

Calls that verify themselves

A wallet check during the call replaces security questions.

Qualifications and access

Licences, training and roles checked at the source, for sites, systems and portals.

Companies and suppliers

Verify a business once. Stop payment-diversion and fake-vendor fraud.

Agents with a person behind them

Scoped, time-limited authority for the agents your people and customers use.

Each of these has a sector version. We choose one together in discovery.

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

One wallet. One unbroken chain of trust. Every agent action traces to a real person who is provably still in control.

One wallet

Verified credentials for people and credentials for their agents sit together, with one recovery path and one audit trail.

One chain of trust

Trusted issuers verify the person. iDen2 links that proof to each agent, with limits that can only narrow.

Alive, not archived

Authority is checked at the moment of use, not once at set-up. It can expire or be withdrawn.

Five modules deploy the full trust stack, no rip & replace.

A modular trust operating system. Deploy the stack or compose individual services.

ISSUANCE · PHENIX®

Credentials Factory

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

VERIFICATION

Trust Mesh

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

INTELLIGENT WALLETS

Custody Wallet

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

AI CONTROL

APoC Engine

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

INTEGRATION

Verification Gateway

Verifies & 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 · CRYSTALS-Dilithium (post-quantum)

The wallet your people and customers carry is the Holder Agentic Wallet, or it can be built into your own app with the white-label SDK.

How it works: issue, hold, verify, and prove who stands behind an agent

1

Issue

A trusted source, such as a bank, employer, university or registry, issues a signed credential after its own checks.

2

Hold

The person keeps it in a wallet. They share only the facts requested and approve with a face or fingerprint.

3

Verify

Your system checks who issued it and whether it is still valid, then decides under your own policy.

4

Delegate

The person gives an agent a signed, limited, time-bound permission. Your system checks it at each use.

Anything above the set limit goes back to the person for approval. Each hand-off can only narrow the permission, never widen it.

What executives get, and how you would measure it

Outcome	What changes	How to measure it
Faster	Customers, staff and partners reuse proof instead of re-submitting it.	Time to onboard, time to grant access, drop-off rate
Safer	Sensitive changes and payments need wallet approval. Agents act within limits.	Account-takeover and payment-fraud cases, reset tickets (baseline first)
Lower effort	Less manual review and fewer calls to issuers or call-centre checks.	Manual-review share, handling time, cost per case
Audit-ready	Each approval and agent action leaves signed evidence.	Audit hours, evidence completeness, disputes resolved
Agent-ready	A named person, scope and expiry behind every agent.	Share of agents with an owner, scope and expiry

No savings figures are quoted here. Targets are set together from your own baseline.

Where iDen2 fits, and where it does not

iDen2 adds

- A credential layer that works across organisations
- Wallet approval for people and a proof of authority for agents
- Connection to Okta, Entra (Azure AD), Ping and similar tools
- Open standards, so you are not locked in
- Signed evidence for audit

iDen2 does not

- Verify who a person is. Trusted issuers do that; iDen2 carries and checks their proof
- Replace your IAM, fraud or engine
- Guarantee compliance or remove fraud. It strengthens the evidence your controls use
- Secure the agent itself. Sandboxing and model safety remain separate
- Promise every organization will accept a credential. Acceptance grows with the network

What you can use now, and what is coming

AVAILABLE TO PILOT TODAY

- Issuing and verifying credentials through standard APIs (OID4VCI, OpenID4VP)
- Selective disclosure: share only the fact requested
- Wallet on iOS, Android and web, plus a white-label SDK
- Core formats: W3C VC, SD-JWT, mDL
- Trust network and developer sandbox
- Verification Gateway to connect existing IAM tools

ON THE ROADMAP

- Full agent registration, scope and action checking (APoC Engine)
- Intelligent wallet: policy engine and credential lifecycle
- Scoped mandates and agent-to-agent trust
- Lossless translation across all seven credential formats
- Credential marketplace
- Payment-bound credentials and loyalty rail
- Liability and insurance framework for agent actions

Status as of October 2026. Confirm availability for your region and use case before committing.

ROADMAP

A glimpse of the road ahead: frequency first, intelligence second, agency third

PHASE 1 · FOUNDATION

2026

- Issuance and verification services hardened for production
- Core formats, trust network, sandbox
- Everyday wallet uses: sign-in, age and eligibility proofs, passes
- Early agent hooks built into the core

PHASE 2 · ENHANCEMENT

2027 H1

- Intelligent wallet: policy engine and lifecycle
- Agent registration and scope (APoC v1)
- Full seven-format translation
- Loyalty rail and payment-bound credentials

PHASE 3 · ECOSYSTEM

2027 H2 and later

- Scoped mandates and agent-to-agent trust
- The five wallet agents in production
- Credential marketplace and interop hub
- Liability and insurance framework

Directional. Timing may change with customer needs, standards and regulation. Early partners help set the order.

A low-risk way to start: one workflow, proven on your own data

1

Discovery

1 to 2 weeks

A short working session to map your identity touchpoints, fraud exposure and compliance questions. We choose one workflow and agree the baseline.

2

Pilot

6 to 10 weeks

Issue and verify in your real workflow, integrated with your stack. Success measures are agreed before we start.

3

Production

After sign-off

Phased rollout across channels and entities. Managed cloud, on-premises or hybrid. Commercial terms agreed after the pilot.

No rip and replace. iDen2 runs beside your existing identity, fraud and KYC tools. You stop if the pilot does not show value on the measures we agreed.

What we ask of you, and what you get

From you

An executive sponsor. One process owner. Access to baseline data on the chosen workflow. A security and legal contact for early review.

From iDen2

A pilot design, working integration support, a named delivery lead, and a clear report of results against the agreed measures.

You keep

The learning, the baseline and the choice. After the pilot you decide to stop, refine or expand.

PICK A STARTING POINT

- **Safer calls and account changes**
- **Faster customer or partner onboarding**
- **Passwordless staff and contractor access**
- **Agent authorisation for one workflow**

Know who’s acting.

The trust layer for the agentic era. Next step: a 60-minute working session to pick one workflow and agree what success looks like.

iden2.com · info@iden2.com

Questions you will hear

Question	Suggested answer
“We already have IAM and SSO.”	Good. Those stay. iDen2 adds portable credentials and proof of authority across organisations and for agents. It connects to the tools you own.
“Does this stop fraud?”	No single control does. We define the threat, test whether stronger evidence helps, and measure it against your baseline.
“Is it compliant with…?”	Compliance depends on the use case, region and your controls. We involve your legal team early and confirm what iDen2 has approved for external use.
“Will others accept the credential?”	Only if they trust the issuer and have compatible tools. We start where one organisation controls the workflow, then grow outward.
“Is this blockchain?”	We lead with the business outcome. We can explain the architecture and any ledger use accurately when it matters to you.
“What if someone loses their phone?”	Recovery is a design choice per use case. We agree the policy with you before any pilot.
“Why do we need this for AI?”	As agents act across systems, you need proof of who authorised them. That sits alongside your AI security controls, not in place of them.