Partner Enablement Toolkit

Digital trust for people, organisations, and AI agents

Purpose

A practical starter pack for technology and digital-solutions partners. It helps partner sales teams identify customer problems, explain iDen2 in plain language, shape use cases, run discovery, and progress toward a measurable pilot. Version 1.0 covers 13 sectors and 152 use-case entries.

Target sectors:

Banking & finance • Telecommunications • Education • E-commerce • Oil & gas • Insurance • Government • Healthcare • NGOs & humanitarian • Workforce & enterprise access • Loyalty • Supply chain & logistics • Travel & hospitality

Version 3.0 | Final | October 2026

Contents

Where to find each part of the toolkit

Section	Page
How to use this toolkit	3
1. Master explainer: What is iDen2?	4
Product maturity guide	5
Use-case map: 13 families across all sectors	6
2. Banking & financial services	8
3. Telecommunications	10
4. Education & professional credentials	12
5. E-commerce & digital marketplaces	14
6. Oil & gas: workforce, contractors, and supply chain	16
7. Insurance	18
8. Government & public programmes	20
9. Healthcare	22
10. NGOs & humanitarian organisations	24
11. Workforce & enterprise access	26
12. Loyalty programmes	28
13. Supply chain & logistics	30
14. Travel & hospitality	32
15. AI trust brief: Who authorised the agent?	34
Pilot blueprint: from interest to evidence	36
Positioning, objections, and guardrails	38
Country-specific localisation checklist	40
Partner and account planning worksheet	41
Initial use-case prioritisation	42
Quick-reference: what every partner should remember	43
About this version (v1.0)	44

How to use this toolkit

This is a general enablement pack, designed before specific partner companies and target accounts have been identified. Use it to align partner teams around a common story, then tailor the relevant sector guide to each partner's existing products, customer relationships and local requirements.

Asset	Who uses it	Purpose
1. Master explainer	All partner sales, product and solution teams	Explain the trust problem and iDen2's role in simple terms.
2. Sector guides (2 to 14)	Sector account managers and solution architects	Connect customer pain points to practical use cases. Each guide has a full use-case library.
3. Use-case map	Sales leads and solution architects	See which use-case families repeat across sectors, and where to lead.
4. AI trust brief (15)	CIOs, CISOs, digital, data and AI leaders	Open a forward-looking conversation about agent identity and delegated authority.
5. Discovery & qualification	Partner sales teams	Identify, qualify, and prioritise opportunities.
6. Pilot blueprint	Partner + iDen2 solution teams + customer	Scope a test with measurable outcomes.
7. Objections & positioning	Sales and executive sponsors	Respond accurately without overclaiming.

Important guardrail: Treat every capability in this pack as a proposed use case until product, engineering, legal/compliance and commercial teams confirm support, integration requirements, regional availability, security evidence, and contractual terms. Do not promise regulatory compliance, fraud elimination, universal acceptance, or specific savings without evidence.

How to read the Lead, Explore and Emerging tags

Tag	Meaning	How to use it
Lead	Clear pain, a credible issuer, and one organisation can control the pilot. These tend to work well as a first conversation.	Suggest as a first pilot after discovery confirms the pain.
Explore	Promising, but the issuer, regulation, integration or second party still needs to be validated with the customer.	Raise in discovery. Do not scope a pilot until the open points are closed.
Emerging	Depends on roadmap capability, an authority, or an ecosystem that does not exist yet.	Discuss as direction. Do not sell as available.

The tags are iDen2's working judgement, not a customer-validated ranking. A partner who knows the account better should challenge them.

Target geography

Initial partner footprint: GCC and the Middle East, with potential expansion into other North African markets.

Pro Tip: Do not assume one regulatory or procurement approach fits all countries. Localise data residency, privacy, identity proofing, e-signature validity, financial-sector rules, government procurement, language, hosting and cross-border transfer requirements with qualified local advisers.

1. Master explainer: What is iDen2?

The simplest explanation

iDen2 provides technology that helps organisations issue, present, and verify digital credentials, and establish trust across systems. Its broader direction includes helping organisations verify the identity and authority of AI agents acting on behalf of people or organisations. It is a decentralised network of verified credentials, so as more users and organisations join the network, the network becomes more useful.

The problem customers recognise

- People and businesses are repeatedly asked to submit the same documents to different organisations.
- Each organisation may build separate workflows to collect, review, store and validate identity or qualification information.
- Documents can be difficult to verify, become outdated, or require manual confirmation with the original issuer.
- Organisations often cannot easily reuse verified information across applications, institutions, or borders.
- As AI agents begin initiating actions, systems need to know not only which software made a request, but who authorised it and what it is allowed to do.

How a credential-based trust flow works

1. The user (the holder of the wallet) completes an initial onboarding by scanning a government-issued ID document, such as a passport, driver's licence or citizen ID.
2. After the person's identity is verified in this trust ecosystem, an organisation can set up its own process to issue a digital credential to its customer, employee, student, organization, or system.
3. The holder stores the credential in the wallet and presents it when asked.
4. A verifier checks the credential's cryptographic validity, issuer, status, and required attributes against its own trust and policy requirements.
5. The verifier uses the result as evidence in its business process, for example onboarding, eligibility, employment verification or access.

Pro Tip: A credential proves that an issuer made a claim; it does not automatically prove the underlying claim was correct. Trust depends on the issuer, evidence, credential lifecycle, verification policy, and the relying party's rules.

What the partner adds

- Integrates iDen2 capabilities into a solution the partner already sells.
- Connects the credential workflow to the customer's applications, processes, and user experience.
- Provides local implementation, configuration, support, and country and sector-specific regulatory knowledge.
- Packages a specific business outcome rather than selling technical standards alone.

What customers are buying

Instead of leading with:	Lead with:
DIDs, VCs, protocols, and wallet architecture	Reduce repeated verification and make trusted information reusable.
A new identity platform	Improve a defined and existing onboarding, credential, or verification workflow.
Blockchain or decentralisation	Interoperability, verifiable evidence, privacy-preserving data sharing, and control.
AI-agent technology	Establish who authorised an agent, its permitted scope, and how its authority can be checked.
“We verify identity”	iDen2 lets organisations issue and check credentials. The issuer and the verifier decide what to trust.

30-second partner pitch “Our digital solutions can include an additional trust layer from iDen2. It helps organisations issue and verify digital credentials and reuse trusted information across supported workflows. That can help simplify business processes such as customer onboarding, employment checks, qualification verification, access management, and document signing. As AI agents become more active in business processes, the same broader trust approach can also support verification of agent identity and delegated authority, subject to the use case and integration.”

Product maturity guide: what to say about what

Partners should know which parts of the platform are available today and which are direction. Confirm the current status with iDen2 product before any customer commitment.

Layer	What it is	Status to assume	How to talk about it
Layer 1: Core utility	Credentials Factory (issue), Holdr Wallet (hold and present), Trust Network (verify and look up issuers). Formats and protocols include W3C Verifiable Credentials, SD-JWT, mDL, OID4VCI and OpenID4VP.	Available. Confirm per configuration and region.	Lead with this. Every pilot in this toolkit starts here.
Layer 2: Intelligent Wallet	A wallet that helps the holder manage, understand and decide on requests.	Roadmap.	Describe as direction. Do not put it in a pilot scope.
Layer 3: Agentic Wallet and APoC	Agent Proof of Control (APoC): signed delegation so an agent can show who authorised it and what it may do. Today's design allows up to two delegation hops, and scope can only narrow.	In development.	Use for AI-trust conversations. Pilot only as a narrow, human-approved test, and only once product confirms.

Use-case map: 13 families across all sectors

The same few patterns repeat in every sector. Learn the families once, then adapt the story.

Family	What it covers	Where it appears
A. Onboarding and reusable verification	A person or business proves who they are once and reuses it.	Bank, Telco, Edu, Ecom, Oil & gas, Insur., Gov, Health, NGO, Staff, Loyalty, Travel
B. Login, account and payment protection	Sign-in, step-up checks and approvals that stop account takeover and payment fraud.	Bank, Telco, Edu, Oil & gas, Insur., Gov, Health, NGO, Staff, Loyalty, Travel
C. Caller and contact-centre verification	A wallet check replaces security questions when someone calls.	Bank, Telco, Edu, Insur., Health, Staff, Loyalty, Travel
D. Physical and site access	Doors, sites and devices open for verified people with the right role.	Telco, Edu, Oil & gas, NGO, Staff, Supply, Travel
E. Qualifications, licences and certificates	Degrees, licences, training and certificates checked at the source.	Edu, Oil & gas, Insur., Health, Staff, Travel
F. Delegation and guardians (people acting for people)	One person acts for another with clear, limited authority.	Bank, Telco, Edu, Health, Travel
G. Digital signing and agreements	Signing and consent tied to a verified person or role.	Bank, Telco, Ecom, Oil & gas, Insur., Health, NGO, Travel
H. Supplier, partner and company verification	Companies, suppliers and partners verified once and reused.	Bank, Telco, Ecom, Oil & gas, Insur., Gov, NGO, Loyalty, Supply, Travel
I. Provenance, custody and traceability	Signed records for goods, parts and handovers.	Oil & gas, Insur., Health, Supply
J. Audit trail and compliance evidence	Signed events that give auditors and regulators clean evidence.	Bank, Telco, Oil & gas, Gov, NGO, Staff, Loyalty
K. Minimum disclosure and eligibility proofs	Prove one fact (age, eligibility) without handing over the whole document.	Bank, Telco, Ecom, Oil & gas, Insur., Gov, Health, NGO, Travel
L. Offline and field verification	Checks that must work with weak or no network.	Oil & gas, Gov, NGO
M. AI agents and machine identity	Agents and machines with a named owner, scope and expiry.	Bank, Telco, Edu, Ecom, Oil & gas, Insur., Gov, Health, NGO, Staff, Loyalty, Supply, Travel

Matrix: number of use cases per family and sector

Colour shows the strongest tag in that cell: green = at least one Lead, amber = Explore, lavender = Emerging. Blank means no use case in this toolkit.

Family	Bank	Telco	Edu	Ecom	Oil & gas	Insur.	Gov	Health	NGO	Staff	Loyalty	Supply	Travel
A. Onboarding and reusable verification	3	1	2	1	1	4	3	2	3	1	1		1
B. Login, account and payment protection	2	3	2		1	1	2	1	1	4	5		2
C. Caller and contact-centre verification	1	1	1			1		1		1	1		1
D. Physical and site access		1	2		1				1	1		1	1
E. Qualifications, licences and certificates			6		1	1		2		1			1
F. Delegation and guardians	1	1	1					1					1
G. Digital signing and agreements	1	1		1	1	1		1	1				1
H. Supplier, partner and company verification	1	1		2	1	2	1		1		1	3	1
I. Provenance, custody and traceability					2	1		1				5	
J. Audit trail and compliance evidence	1	1			2		1		1	2	1		
K. Minimum disclosure and eligibility proofs	1	1		2	1	1	3	1	1				2
L. Offline and field verification					2		1		1				
M. AI agents and machine identity	2	2	1	1	1	1	1	1	1	1	1	1	1

What this tells a partner: family B (login and payment protection) and family C (caller verification) carry the most Lead tags, because the pain is clear and one organisation can run the pilot. Family A (onboarding) is mostly Explore, because it depends on issuers and regulators. Families I, L and M are mostly Explore or Emerging, because they need other parties, or roadmap capability, to deliver value.

2. Banking & financial services

From repeated checks to reusable financial trust

The business problem

Banks, lenders, payment providers, and fintechs must establish customer and business identity, conduct due diligence, verify documents, and maintain evidence. Repeated collection, manual review, and fragmented integrations can increase cost, lengthen the workflow, and create friction for customers. Scams where the customer approves the payment, and customer AI agents, add two newer problems.

Priority use cases

Use case	How iDen2 could fit
Customer onboarding	Present and verify supported identity or KYC-related credentials as one evidence source in the onboarding workflow.
Business KYC / KYB	Verify company registration, licenses, beneficial ownership-related attestations or authorized-representative credentials where an appropriate issuer and evidence process exist.
Loan and account agreements	Integrate digital-signing capabilities into loan, account-opening, or service-contract workflows, subject to local legal validity and signing requirements.
Customer eligibility and rewards	Verify selected attributes or eligibility credentials for product/platform access, offers, or loyalty benefits, using data minimization where supported.
Call-centre and account-takeover protection	Replace knowledge questions with a wallet-based check before sensitive changes; keep existing fraud systems in place.
AI-enabled finance	Explore signed delegation and scoped authority for agents preparing or initiating supported financial workflows; retain existing payment, fraud, and approval controls.

Partner discovery question: Which onboarding, lending, or servicing workflows repeatedly collect evidence that could be issued by a trusted source and verified digitally?

Pro Tip: A reusable credential does not automatically satisfy every KYC/AML, sanctions, suitability, source-of-funds or recordkeeping obligation. The bank remains responsible for its regulatory decisions and controls.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Government ID source, national digital ID, or another bank	Customer	Bank, lender or fintech
Company registry or licensing authority	Company officer or authorised signer	Bank (business onboarding)
Bank	Customer or business	Partner, merchant or the bank's own call centre

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (13 use cases)

Use case	What it does	Friction today	Start	Family
Agentic Banking Authority	Customers delegate limited tasks to AI agents	Agents use shared logins or full-access tokens	**Emerging**	M
Account Takeover Prevention	Stop logins that are valid but not the owner	Stolen passwords and SIM swaps defeat SMS codes	**Lead**	B
Business & Commercial KYC	Verify companies, officers and signers once	Corporate onboarding takes weeks of document chasing	**Explore**	H
Wire & Payment Fraud Defense	Bind high-risk payments to a live approval	Business email compromise changes payee details	**Explore**	B
Call Center Authentication	Replace knowledge questions with a wallet check	Agents spend the first minute on security questions	**Lead**	C
Wealth & Advisory Delegation	Let advisers and family act with clear limits	Power of attorney is paper held in a file	**Explore**	F
Treasury & Business Agents	Authorize finance bots and ERP agents	Treasury bots hold long-lived API keys	**Emerging**	M
Regulatory Audit Trail	Show who approved what, and why	Evidence is spread over logs, emails and call notes	**Explore**	J
Cross-Institution Reusable KYC	Verify once, reuse with consent	Customers repeat KYC at every bank and fintech	**Explore**	A
Stablecoin & Digital Asset Compliance	Bring identity to on-chain transfers	Wallet addresses say nothing about who owns them	**Emerging**	A
Customer onboarding	Use supported credentials as one evidence source in digital onboarding	The same documents are collected and reviewed again at each institution	**Explore**	A
Loan and account agreements	Digital signing inside loan, account-opening and service-contract flows	Paper or e-sign steps sit outside the identity check	**Explore**	G
Customer eligibility and rewards	Prove a selected attribute for offers or benefits without sharing more	Eligibility is proven with full documents or self-declaration	**Lead**	K

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Less repeated collection and checking of the same evidence	• Cost per completed onboarding
• Faster handling of eligible onboarding cases	• Median onboarding time
• Lower manual-review effort where a credential can be accepted	• Manual-review percentage
• Stronger protection for high-risk changes such as payee, address and device changes	• Customer drop-off rate
• Improved audit evidence and clearer credential lifecycle controls	• External document verification time
• Potential new embedded trust services for the partner	• Signing completion time
	• Call handling time before sensitive requests
	• Account-takeover and payee-change fraud cases (baseline first)

3. Telecommunications

Trust across subscriber, enterprise, and digital services

The business problem

Telcos verify subscribers, manage account changes and onboard enterprise customers. They also sell connectivity, cloud, security, and digital platforms to other sectors. Identity-dependent workflows may be fragmented across channels and products, and attackers target the weak points: SIM swaps, port-outs, remote eSIM downloads and call-centre social engineering.

Priority use cases

Use case	How iDen2 could fit
Subscriber onboarding	Use supported credentials or verified attributes as evidence in digital onboarding, subject to national SIM-registration rules and operator policy.
SIM-swap and port-out protection	Require a wallet approval before a SIM change or port-out, alongside the operator's existing fraud controls.
Enterprise customer onboarding	Verify business and authorized-representative credentials before provisioning enterprise services.
Document and contract signing	Integrate signing into new subscriptions, enterprise contracts, service changes or renewals, subject to local law and the specific signing method.
Portals and physical access	Verify role, employment, training, entitlement or access credentials at supported portals or entry points, integrated with the operator's access system.
AI and automated service operations	Explore verifiable delegation for agents that access customer-service or provisioning workflows; retain network security and API access controls.

Partner discovery question: Which identity or document checks slow down subscriber onboarding, SIM and account changes, enterprise provisioning, or the digital solutions you sell to other businesses?

Pro Tip: Credential verification does not replace SIM-registration obligations, telecom security, network authentication, fraud systems, or operator-specific identity-proofing requirements. Network-API and roaming ideas depend on industry programmes and partner agreements; treat them as exploratory.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Government ID source or national digital ID	Subscriber	Operator (onboarding, SIM change, call centre)
Company registry	Company's authorised representative	Operator enterprise team
Operator	Subscriber or business user	Partner service or network-API buyer

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (13 use cases)

Use case	What it does	Friction today	Start	Family
SIM Swap & Port-Out Protection	No wallet approval, no SIM change	Attackers use breached data in stores and calls	**Lead**	B
eSIM Provisioning Trust	Safe remote activation	Remote eSIM download is easy to abuse	**Explore**	B
Subscriber Onboarding & KYC	Verify once, onboard in minutes	Fake applications get through	**Explore**	A
Agentic Customer Care	AI care agents with limits	AI care agents have wide system access	**Emerging**	M
Call Center Authentication	Replace the security quiz with a wallet check	Agents run a script of personal questions	**Lead**	C
Roaming & International Authentication	Trust that travels	Travellers face new checks abroad	**Explore**	B
Business & Enterprise Line Management	Who may change which business line	Company lines are changed by anyone with an email	**Explore**	F
Network API & CAMARA Monetization	Sell trust as a service	Buyers cannot see the consent behind a signal	**Emerging**	K
IoT & Device Identity	Know which device is on the network	IoT SIMs are cloned or moved to other devices	**Emerging**	M
Regulatory Audit Trail	Prove each change was authorized	Evidence sits in several systems	**Explore**	J
Enterprise customer onboarding	Verify business and authorised-representative credentials before provisioning	Company documents and signatory authority are checked by hand	**Explore**	H
Document and contract signing	Signing built into subscriptions, enterprise contracts and renewals	Signing sits outside the identity check	**Explore**	G
Portals and physical access	Role or entitlement credentials at partner portals and operator sites	Separate logins and badges for staff, contractors and partners	**Explore**	D

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Simpler identity-dependent service journeys	• Subscriber onboarding time
• Potential reduction in repeated document review	• Manual verification rate
• Stronger protection for SIM change, port-out and eSIM provisioning events	• Enterprise provisioning lead time
• New embedded trust features for enterprise customers, including digital signatures tied to a verifiable credential	• Contract completion rate
• More consistent evidence across channels	• Cost per identity-dependent service event
• A differentiated digital trust offering beyond connectivity	• SIM-swap and port-out fraud cases (baseline first)
	• Partner attach rate / new revenue

4. Education & professional credentials

Credentials that learners can present and employers can verify

The business problem

Universities, vocational providers, training organisations, and professional bodies issue qualifications that learners later need to prove to employers, licensing bodies, or other institutions. Verification can depend on manual requests, PDFs, or separate portals. Higher education also carries fake applicants, exam impersonation, and international-student paperwork that a student credential can help with.

Priority use cases

Use case	How iDen2 could fit
Digital diplomas and certificates	Issue supported verifiable credentials for qualifications, course completion, and training.
Employment and licensing checks	Enable a graduate or professional to present credentials for verification by an employer or licensing body.
Continuing professional development	Issue training and renewal credentials with relevant dates and status information.
Campus access and student benefits	Verify student status or entitlement for access, discounts, facilities, or partner rewards where appropriate.
Admissions and registrar protection	Bind applicants and students to a verified identity so fake applications and call-centre fraud are harder.
AI-assisted recruitment	Provide stronger evidence of qualifications to recruiting workflows; separately govern the use of AI in candidate evaluation.

Partner discovery question: How do graduates currently prove their qualifications, and how much staff time is spent responding to external verification requests?

Pro Tip: The credential does not establish academic quality or equivalence by itself. Issuer authority, accreditation, qualification frameworks and receiving-body acceptance still matter. Fraud-detection and exam-integrity use cases support, but do not replace, the institution's own integrity process.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
University, college or training provider	Learner or alumnus	Employer, licensing body or another institution
Professional body or regulator	Professional	Employer or client
Education ministry or national ID source	Applicant or student	Admissions office

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (15 use cases)

Use case	What it does	Friction today	Start	Family
Admissions & ghost-student prevention	Bind applicants to a verified person before a student record exists	Bots and synthetic applicants pass document-based checks	**Explore**	A
Enrollment & the golden student record	One verified identity across admissions, registrar, aid and housing	Each office holds a slightly different student record	**Explore**	A
Academic integrity & exam identity	Confirm who is taking the exam, and who authored the work	Remote exams rely on webcams and honour codes	**Explore**	B
Campus access & housing	Student ID in the wallet for dorms, library, gym and events	Cards are lost, cloned and shared	**Lead**	D
Financial aid & disbursement verification	Re-confirm the recipient is a live, enrolled person at disbursement	Aid reaches fake or stolen identities	**Explore**	B
International visa & status compliance	Visa, enrollment and work-permission status as credentials the office can check	Status is tracked by hand across offices (map to local sponsor rules)	**Explore**	E
Study abroad & exchange mobility	One exchange credential recognised by partner institutions	Every partner re-verifies the same student	**Explore**	E
Transfer credit & credit mobility	Signed course and grade credentials that receiving institutions can verify	Transcript review is repeated and inconsistent	**Explore**	E
Research collaboration & lab access	Role and affiliation credentials for labs and datasets	Shared logins to sensitive labs and data	**Explore**	D
Alumni credentials & diploma authenticity	Degree and transcript as a credential the alumnus holds	Employers verify by phone, fax or email to the registrar	**Lead**	E
Registrar & contact-centre verification	Wallet push replaces security questions on calls	Callers are checked with data that is often breached	**Lead**	C
Accommodations, minors & guardian delegation	Scoped authority for guardians and accommodation credentials	Paper forms and repeated proof each term	**Explore**	F
Employment and licensing checks	Graduate or professional presents credentials to an employer or licensing body	Manual verification requests and separate portals	**Lead**	E
Continuing professional development	Training and renewal credentials with dates and status	Renewals tracked in spreadsheets and certificates	**Lead**	E
AI-assisted recruitment and student agents	Stronger evidence for recruiting tools; scoped mandates for advising or application agents	No standard way to show which agent acts for whom	**Emerging**	M

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Reduced administrative handling of verification requests	• Average qualification verification time
• Faster checks for employers and licensing bodies	• Requests handled manually
• Improved portability of qualifications	• Cost per verification
• Fewer fake applications and fewer identity-driven disbursement problems	• Credential issuance volume
• More efficient alumni and credential services	• Employer/verifier adoption
• Potential cross-institution credential ecosystems	• Credential correction and revocation handling time
	• Applications flagged as fraudulent (baseline first)

5. E-commerce & digital marketplaces

Trust between platforms, sellers, buyers, and AI commerce agents

The business problem

Marketplaces onboard merchants and suppliers, assess eligibility, validate business documents, and manage fraud and disputes. As the ecosystem grows, manual checks and platform-specific records can make expansion costly.

Priority use cases

Use case	How iDen2 could fit
Customer verification	Verify customer information, including customer address, mobile number, and email address for improved customer experience.
Customer eligibility and rewards	Verify selected attributes or eligibility credentials for platform access, offers, or loyalty benefits, using data minimization where supported.
Seller and merchant onboarding	Verify business registration, licenses, or other supported business credentials from trusted issuers.
Supplier qualification	Present certifications, permits, insurance evidence, or other credentials required by a marketplace or buyer.
Age or eligibility checks	Verify a required attribute without exposing additional information where the solution supports this and local law permits.
Digital agreements	Integrate signing into merchant terms, supplier agreements, or platform contracts, subject to legal requirements.
AI shopping and procurement agents	Explore signed, scoped, and revocable delegation for agents acting for a consumer or business, alongside transaction limits, payment controls, and dispute processes.

Partner discovery question: Which seller, supplier or buyer claims must your platform verify repeatedly, and which trusted parties could issue the evidence?

Pro Tip: Credentials do not eliminate marketplace fraud or guarantee seller performance. They must be combined with risk scoring, payment controls, monitoring, and dispute management. Note: there is no dedicated e-commerce solution deck yet; the use cases above come from toolkit v0.2 and should be tested before wide use.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Business registry or licensing authority	Merchant or supplier	Marketplace
Government ID or mobile operator	Customer	Marketplace or retailer
Certification body or insurer	Supplier	Buyer or marketplace

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (7 use cases)

Use case	What it does	Friction today	Start	Family
Customer verification	Verified address, mobile number and email for smoother checkout	Unverified contact details cause failed deliveries and fraud checks	**Lead**	A
Customer eligibility and rewards	Prove a selected attribute for offers or benefits	Eligibility is claimed, not proven	**Lead**	K
Seller and merchant onboarding	Business registration and licences from trusted issuers	Manual document review slows seller growth	**Explore**	H
Supplier qualification	Certifications, permits and insurance evidence presented as credentials	Each marketplace or buyer re-collects the same evidence	**Explore**	H
Age or eligibility checks	Prove a threshold without sharing the birth date	Full ID is shown to confirm a yes or no	**Lead**	K
Digital agreements	Signing built into merchant terms and supplier contracts	Contract steps sit outside the identity check	**Explore**	G
AI shopping and procurement agents	Signed, scoped and revocable authority for agents buying for a person or business	Bots and buyer agents look the same to the platform	**Emerging**	M

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Potentially faster customer verification and improved user experience	• Customer drop rate
• Potentially faster merchant and supplier onboarding	• Merchant onboarding time
• Reduced duplicate document handling	• Percentage of cases requiring manual review
• Better evidence for platform eligibility decisions	• Cost per seller verification
• New trust services the partner can embed	• Supplier approval lead time
• A path to support agent-mediated commerce	• Dispute-resolution time
	• Agent transaction exception rate

6. Oil & gas: workforce, contractors, and supply chain

Trusted workforce and supplier credentials across complex operations

The business problem

Oil and gas operators and contractors work across sites, subcontractors, jurisdictions, and high-consequence environments. They need to check worker identity, qualifications, safety training, permits, supplier credentials, and contractual evidence. Remote and offshore sites, shared operating-technology accounts, and growing use of automation add further identity questions.

Priority use cases

Use case	How iDen2 could fit
Employment and contractor verification	Verify supported identity, employer, role, or engagement credentials during onboarding and mobilization.
Safety and competency credentials	Issue and verify training, certification, medical-clearance, or competency attestations where the issuer and privacy/legal basis are appropriate.
Site and portal access	Check role, training, or entitlement credentials as one input to physical or digital access-control decisions.
Supplier and supply chain verification	Verify business registrations, certifications, insurance evidence, inspection attestations, or authorized-representative credentials.
Contract execution	Integrate digital signing for contracts, work orders, permits, or supplier agreements, subject to the legal and operational requirements.
AI agents in procurement and operations	Explore agent identity and scoped delegation for agents that source suppliers, request quotations or prepare orders, with human approvals and operational safety controls.

Partner discovery question: Which workforce or supplier checks are repeated across sites, contractors, and projects, and who is trusted to issue the underlying evidence?

Pro Tip: A digital credential is not a substitute for safety management, site induction, permit-to-work controls, occupational health processes, or operator-specific approval. Sensitive employment and health data require strict minimisation and access controls. Do not describe the product as meeting any named cyber-security or local-content rule until confirmed.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Training provider, medical assessor or certification body	Worker	Gate, permit desk or mobilisation system
Contracting company	Worker or company	Operator
Manufacturer or inspection body	Equipment or part (credential travels with it)	Goods-receipt or maintenance team

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (14 use cases)

Use case	What it does	Friction today	Start	Family
Contractor mobilization	Reusable worker credentials requested for each contract	Every contract restarts document collection from zero	**Lead**	A
Competency & certification	Training providers issue safety tickets as signed credentials	Certificates are images and cards that are easy to forge	**Lead**	E
Site & facility access	Access decision computed from current credentials at the gate	A badge proves past enrolment, not current clearance	**Lead**	D
Permit to work & isolation	Permit signatures bound to a verified person with the right competency	Signatures are wet ink or shared logins	**Explore**	J
OT / ICS access governance	Individual, role-scoped, time-limited access to control systems	Shared and default credentials persist on legacy systems	**Explore**	B
Remote & offshore access	Credentials checked on the device with no live connection	Online checks fail where connectivity is weak	**Explore**	L
Supplier & parts provenance	Manufacturers issue material and test certificates as signed credentials	Editable PDFs and counterfeit parts	**Explore**	I
In-Country Value attestation	Nationality, qualification and supplier status evidence from authoritative sources	Local-content scores rest on self-declaration and sampling	**Explore**	J
Cargo & custody transfer	Signed quality, quantity and custody records	Shipping documents are forgeable paper	**Explore**	I
Emergency response & muster	Live personnel-on-board record from verified entries	Muster lists are paper and reconciliation takes hours	**Explore**	L
Joint venture data exchange	Partners verify each other's credentials without sharing databases	Each partner keeps separate worker records	**Explore**	K
AI agent authorization	Scoped, time-limited authority for agents acting on assets	Agents run on API keys and shared service accounts	**Emerging**	M
Supplier and company verification	Registration, certification and insurance credentials from the issuer	Prequalification platforms hold company-level evidence only	**Explore**	H
Contract execution	Signing for contracts, work orders and permits	Contract and permit steps sit outside the identity check	**Explore**	G

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Less repetitive checking across contractors and projects	• Time to mobilize workers
• Faster mobilization when credentials are accepted	• Credential review time
• Clearer evidence of competency and supplier status	• Expired credential exceptions
• More efficient audit preparation	• Supplier onboarding lead time
• Individual, time-limited and attributable access to sensitive systems	• Manual audit preparation hours
• Potential interoperability across operators, contractors, and service providers	• Contract turnaround time
	• Gate verification time
	• Shared or default accounts remaining on in-scope systems

7. Insurance

Trusted evidence across policyholder, broker, provider, and claims workflows

The business problem

Insurers and brokers collect identity, business, licence, asset, and incident documents during onboarding, underwriting, policy servicing, and claims. Verification can involve multiple external parties and manual follow-up. Easy-to-fake photos and documents, impersonation of adjusters after a disaster, and caller fraud add pressure.

Priority use cases

Use case	How iDen2 could fit
Policyholder onboarding	Use supported credentials as evidence in identity and business onboarding workflows.
Broker and intermediary credentials	Verify licensing, appointment, employment, or authority credentials where trusted issuers and appropriate status checks exist.
Commercial insurance and supplier risk	Verify company registrations, certifications, or insurance evidence in relevant business workflows.
Claims and supporting documents	Verify the origin and integrity of supported documents or attestations; use as one input rather than an automatic claims decision.
Digital signing	Integrate signing into policy documents, broker agreements, or renewals, subject to local legal requirements.
AI-assisted underwriting or claims	Use verifiable evidence and define delegated authority for AI-enabled workflows, with human oversight and existing decision controls.

Partner discovery question: Which external documents or intermediary credentials cause the most delay in onboarding, underwriting or claims?

Pro Tip: Credential validity does not determine coverage, insurable interest, risk, liability, or claim entitlement. Insurance regulation, underwriting rules, and claims governance remain in force. Signed evidence shows who issued a document, not that the event it describes really happened.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Government ID source or bank	Policyholder	Insurer or broker
Garage, clinic, appraiser or registrar	Claimant (evidence travels with the claim)	Insurer claims team
Regulator and the insurer	Producer, broker or adjuster	Customer, insurer systems

How to open the conversation: “We are looking at ways to make trusted information easier to issue, present, and verify across your existing digital workflows. Could we map one process where repeated document collection or verification creates measurable cost, delay, or risk, and assess whether a credential-based approach could improve it?”

Full use-case library (13 use cases)

Use case	What it does	Friction today	Start	Family
Onboarding & reusable KYC	Verified identity at quote and bind, reused for later products	Document uploads and manual review; customers abandon the quote	**Lead**	A
Omnichannel authentication	One credential for app, web, phone and in person	Passwords for the portal, questions on the phone, documents in person	**Lead**	B
Contact-centre verification	Wallet push replaces security questions	Callers are checked with data that is often breached	**Lead**	C
Claims first notice of loss (FNOL) identity	Claim opened from the wallet with verified identity and policy data	Identity is re-proven with the same weak methods; intake is incomplete	**Explore**	A
Claim evidence authenticity	Estimates, reports and valuations signed by the issuer; photos with device attestation	Photos and documents can be faked with AI tools	**Explore**	I
Verified field ecosystem	Adjusters, contractors and repair shops hold credentials the customer can check	Impersonators visit victims after a disaster	**Explore**	H
Life: beneficiary claims	Death certificate and beneficiary identity as credentials	Beneficiaries chase paper certificates and notarised ID	**Explore**	A
Health: member & provider ID	Member and provider credentials checked at care and at claim time	Cards are shared; provider checks are periodic paperwork	**Explore**	A
Producer & broker licensing	Licence and appointment credentials checked at each quote and sale	Licences tracked in spreadsheets across lines and regions	**Lead**	E
Privacy-first personalisation	Prove an attribute or threshold without sharing the raw record	Pricing needs sensitive data that must then be stored	**Explore**	K
Commercial insurance and supplier risk	Company registration, certification and insurance evidence	Business documents chased by email	**Explore**	H
Digital signing	Signing for policies, broker agreements and renewals	Signing is separate from the identity check	**Explore**	G
AI agents for policyholders and insurers	Scoped mandates for agents that quote, file or adjudicate	Insurers must treat agent traffic as suspect	**Emerging**	M

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Less manual document chasing	• Time to bind a policy
• Faster processing of eligible cases	• Time to verify an intermediary
• Better evidence provenance	• Document follow-up rate
• More efficient intermediary verification	• Claims processing time
• Potential reduction in duplicate verification work	• Manual review hours
• A way to tell a real adjuster or partner from an impersonator	• Signing completion rate
	• Caller verification time
	• Quote-to-bind completion rate

8. Government & public programmes

Verified identity with dignity and privacy, from application to payment

The business problem

Public programmes lose money and trust when the person on file is not who they seem, when a changed address or name cannot be checked across separate agency databases, and when benefits keep paying after a life event. Genuine citizens also lose out: benefits expire or are cut off because evidence cannot be shared easily between agencies. This section is written to be usable anywhere. Programme names in the older version were US-specific and have been generalised; map them to the local equivalents.

Priority use cases

Use case	How iDen2 could fit
Benefits eligibility verification	Check an applicant's credential against a real, living, currently eligible person before benefits start.
One citizen portal login	One wallet credential for several agency services, alongside the government's existing national digital identity where one exists.
Caseworker and contractor access governance	Scoped, time-limited case-file access for verified staff and contractors, withdrawn when the engagement ends.
Cross-agency sharing with minimum disclosure	Prove an eligibility fact to another agency without handing over the underlying documents.
Programme-specific eligibility credentials	Food and nutrition support, family and housing support, child programmes and public health coverage, each as a credential issued by the programme.
Sensitive-identity cases	Design patterns for people whose location or identity must stay protected. Needs legal and safeguarding review before any pilot.

Partner discovery question: Where does the programme lose the most time or money because one agency cannot easily confirm what another already knows about a person?

Pro Tip: Do not claim government security certifications, compliance, or specific response times unless iDen2 has confirmed them for that country. Procurement rules, sovereign hosting, and the country's own digital identity scheme usually decide the route. Sensitive-identity cases need legal and safeguarding review and should not be offered casually.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
National ID authority or civil registry	Citizen or resident	Any participating agency
Programme agency (benefits, housing, health coverage)	Recipient or household	Provider, caseworker or another agency
Agency that employs or contracts the caseworker	Caseworker or contractor	Case-management system

How to open the conversation: “Many agencies check the same facts about the same person again and again. Could we map one programme where a verified fact issued by one agency could be accepted by another, so citizens do not repeat the proof and caseworkers spend less time re-checking?”

Full use-case library (12 use cases)

Use case	What it does	Friction today	Start	Family
Benefits eligibility verification	Applicant's credential checked against a real, living, eligible person	Applications under synthetic or stolen identities clear paper checks	**Lead**	A
Continuous eligibility recertification	Status stays proven for as long as benefits flow	Moves, deaths and income changes go unseen for months	**Explore**	A
Unemployment claim verification	Claimant proven to be a real, live person before the first payment	Fraud is found by investigation months after payment	**Explore**	A
One citizen portal login	One credential for many agency services	A dozen logins and passwords to remember and reset	**Lead**	B
Caseworker & contractor access governance	Case-file access scoped to a verified person and time period	Access outlives the engagement	**Lead**	B
Cross-agency data sharing, minimum disclosure	One agency proves a fact to another without sharing records	Agencies copy full documents or databases	**Explore**	K
Life-event & death-reporting integrity	Verified life events stop or change benefits at once	Updates depend on periodic data matching	**Explore**	J
Provider & vendor payment integrity	Providers billing a programme verified as licensed, operating entities	Billing from entities that should not be paid	**Explore**	H
Offline verification in the field	Identity and eligibility checked with no live connection	Rural clinics, mobile units and disaster response lose connectivity	**Explore**	L
AI agent authorization	Each agent assisting staff or citizens bound to a named human owner	Agents act with no clear owner or limits	**Emerging**	M
Programme-specific eligibility credentials	Food, housing, family, child and health-coverage credentials issued by the programme	Each programme re-verifies the same household	**Explore**	K
Sensitive-identity cases	Prove eligibility without revealing a protected location or identity	Records can expose people who must stay hidden	**Emerging**	K

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Caseworker-bound authorisation and a clear due-process audit trail	• Eligible citizens successfully enrolled
• Fewer applications cleared on false or synthetic identities	• Time from application to verified eligibility
• Faster, simpler enrolment for people who genuinely qualify	• Share of cases needing manual review
• Benefit or access changes that take effect when a verified life event is recorded	• Improper payments found and recovered (baseline first)
• Less personal data copied between agencies	• Time from a life event to benefit change
• Records of who decided what, and when	• Caseworker minutes per recertification
	• Personal data fields exposed in verifications

9. Healthcare

Trusted evidence across patient access and clinical operations workflows

The business problem

Each part of a health system verifies identity its own way, and each of those ways is a weak point for fraud, denied claims and delay. Wrong-patient records, credentialing delays, paper consent and unaccountable AI tools all trace back to one question: who exactly is this person, and what are they allowed to do, at this moment of care?

Priority use cases

Use case	How iDen2 could fit
One record	Enrol the patient once with a verified identity credential so registration starts from a strong match instead of a name search.
Verify callers	Send a wallet check during the call and step up for high-risk requests such as records release or an address change.
Live proof of coverage	A member credential signed by the payer, kept current when coverage changes.
Days, not months, for credentialing	Boards, schools and regulators issue licences and certifications to the clinician's wallet for the medical staff office to verify.
Signed clinical facts	Referrals and clinical attestations arrive as credentials signed by the ordering clinician.
Consent with a receipt	The patient signs a scoped, time-bound consent in the wallet, and both sides hold a record of it.

Partner discovery question: Where in registration, contact-centre, coverage, credentialing, or consent does the wrong person, a stale record, or a missing proof cost time, money, or patient safety today?

Pro Tip: Health data is among the most sensitive data a credential can touch. A credential does not replace clinical judgement, consent law, e-prescribing rules, or the hospital's own records policy. Do not say the product is HIPAA-compliant or meets any other named health-privacy law unless iDen2 has confirmed it; privacy law differs by country.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Hospital or clinic	Patient	Hospital, clinic, payer or pharmacy
Medical board, school or regulator	Clinician	Medical staff office, payer or pharmacy
Insurer or health plan	Member	Provider front desk

How to open the conversation: “Imagine one trusted proof for a patient or clinician that works at registration, in the contact centre, at the front desk and in the billing cycle. Could we map one of those workflows where the wrong person, a stale record or a repeated check costs time or money, and test whether a credential-based approach improves it?”

Full use-case library (11 use cases)

Use case	What it does	Friction today	Start	Family
Patient registration & matching	Verified identity credential bound to the record	Name and birth-date matching creates duplicates and overlays	**Lead**	A
Portal & telehealth sign-in	Passwordless, biometric-bound sign-in with step-up for sensitive views	Resets, lockouts and unclear who is on camera	**Lead**	B
Contact-centre verification	Wallet push before health information is discussed	Callers are checked with data that is often breached	**Lead**	C
Coverage & eligibility at care	Payer-signed coverage credential checked at the front desk	Shared or stale member cards; keying errors	**Explore**	A
Provider credentialing	Licences and certifications issued as credentials and reused by hospitals and payers	Primary-source checks repeat for every hospital and payer	**Explore**	E
Prior authorisation & referrals	Clinician-signed facts that payers can verify	Documents cannot be trusted, so everything is re-reviewed	**Explore**	I
Consent & records release	Scoped, revocable consent with a receipt on both sides	Paper forms, fax and no reliable proof of who agreed to what	**Lead**	G
e-Prescribing identity	Prescriber licences and biometric step-up on controlled orders	Stolen prescriber credentials; manual audit trails	**Explore**	E
Caregiver & guardian delegation	Scoped authority for family, guardians and proxies	Shared passwords and paperwork re-proven at every site	**Explore**	F
Clinical trials & research	Prove eligibility without opening the chart; one person, one enrolment	Duplicate subjects; weak consent provenance	**Explore**	K
Clinical AI agents	Scoped mandates for documentation, prior-authorisation and patient assistants	No way to show which agent touched health data and under whose authority	**Emerging**	M

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Fewer registration errors and duplicate records	• Duplicate-record rate
• Less time lost to caller verification	• Caller verification time
• Fewer denials caused by identity or coverage errors	• Denials linked to identity or coverage data (baseline first)
• Faster clinician onboarding where credentials are accepted	• Clinician onboarding time
• Cleaner, auditable consent	• Prior-authorisation turnaround
• A clear record of what each AI tool was allowed to do	• Share of consents captured digitally
	• Wrong-patient events (baseline first)

10. NGOs & humanitarian organisations

Reaching the right person once, with the least data collected

The business problem

Humanitarian and development organisations register people, deliver aid, manage field staff and report to donors, often with weak networks and fragile documents. The same person can be registered twice, aid can reach the wrong hands, and reports rest on manual tallies. At the same time, the people they serve are often at risk, so collecting more data than needed is itself a danger.

Priority use cases

Use case	How iDen2 could fit
Beneficiary enrolment and deduplication	Bind one verified identity to one registration so duplicates and fake entries are harder to create.
Cash and voucher disbursement	Confirm at payout that the right, enrolled person received the aid, with a record the donor can audit.
Field worker and volunteer access	Issue role and training credentials so sites and systems can check who is who and what they may do.
Offline verification	Support checks in places with no network, where the exact offline behaviour has been confirmed for the product configuration.
Donor reporting and fund traceability	Provide verifiable records of who was reached, without exposing their identity.
Data minimisation for at-risk people	Prove eligibility with the least possible data, so a registry is not a list of targets.

Partner discovery question: Where does your organisation lose money, time or trust because it cannot confirm who a person is, whether they were already served, or who is acting for whom?

Pro Tip: Be honest about fit. NGOs rarely buy on their own budget; funding usually comes from donors and agencies, and procurement is slow. Biometric and refugee-registration use cases carry protection, consent and legal risk, and need legal and safeguarding review before they are offered. Never promise offline operation or deployment at scale until confirmed.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
UN agency, government registry or the NGO itself	Beneficiary	NGO distribution point, partner agency or payment provider
NGO	Field worker or volunteer	Site, warehouse or case-management system
Lead NGO or donor	Sub-grantee or implementing partner	Donor or auditor

How to open the conversation: “Many aid programmes struggle to be sure the right person is served once, and to show donors that. Could we map one programme where duplicate registration or manual reconciliation costs money, and test whether a credential-based approach helps while collecting less data?”

Full use-case library (11 use cases)

Use case	What it does	Friction today	Start	Family
Beneficiary Enrollment & Deduplication	One person, one registration	Duplicate and fake enrollment goes undetected	**Explore**	A
Cash & Voucher Disbursement Verification	Prove the right person got paid once	Agents and brokers take cuts or pay the wrong person	**Explore**	B
Field Worker & Volunteer Access	Know who is on your site and what they may do	Badges are copied or lent	**Lead**	D
Offline Verification in Remote Settings	Checks that work with no network	Online verification fails in the field	**Explore**	L
Donor Reporting & Fund Traceability	Show donors who was reached	Reports rely on manual tallies	**Explore**	J
Cross-Agency Deduplication	Stop the same household being funded twice	Agencies cannot share beneficiary lists	**Emerging**	A
Partner & Sub-Grantee Verification	Verify who you fund down the chain	Sub-grantees are checked by paperwork	**Explore**	H
Protection-Sensitive Data Minimization	Prove eligibility without exposing the person	Registration collects far more than needed	**Explore**	K
Refugee & Displacement Registration	Identity that survives the journey	Documents are lost, destroyed or never issued	**Emerging**	A
AI Agent Authorization	Let software help, within strict limits	Chatbots and case tools touch sensitive data	**Emerging**	M
Grant and partnership agreements	Digital signing of agreements with donors and implementing partners	Agreements are signed on paper across several time zones	**Explore**	G

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Fewer duplicate and fake registrations	• Duplicate-registration rate (baseline first)
• Better evidence that aid reached the intended people	• Time to enrol a household
• Less manual reconciliation for donor reports	• Disbursement exceptions and disputes
• Clearer control of who staff, volunteers and partners are	• Staff and volunteer onboarding time
• Less personal data collected and held per person	• Hours spent preparing donor reports
• A safer base for any use of AI tools on case data	• Share of checks completed offline
	• Personal data fields collected per beneficiary

11. Workforce & enterprise access

One verified identity for people, doors, systems and agents

The business problem

Every organisation has employees, contractors, vendors and, increasingly, software agents who need access. Passwords are phished, contractor onboarding takes days, leavers keep access in forgotten systems, and the service desk can be talked into resets. Badge systems and IT access sit apart. This sector is also a good starting point for partners that already sell identity, security or managed IT.

Priority use cases

Use case	How iDen2 could fit
Passwordless employee login	Use wallet-based, phishing-resistant sign-in alongside the existing identity provider.
Contractor onboarding and time-bound access	Verify a contractor's identity and qualifications once, and grant access that ends with the contract.
Service desk and recovery protection	Require a wallet check before password resets and device recovery.
Converged physical and digital access	Use one credential for doors and applications, integrated with the existing access-control system.
Offboarding and revocation	Cut access quickly across connected systems, within the status-check policy window the customer sets.
AI agent authorisation	Name a human owner and a scope for every agent, with expiry and audit evidence.

Partner discovery question: Which sign-in, onboarding or recovery step do your staff and contractors struggle with, and where does access outlive the person or the contract?

Pro Tip: iDen2 does not replace the identity provider, MFA, privileged-access tools or the badge system. Position it as the credential layer that sits with them. Do not claim instant revocation; the speed depends on the verifier's status-check policy. Check employment law and works-council rules before using biometrics or monitoring.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Employer or HR system	Employee	Applications, doors and service desk
Contractor's company or training body	Contractor	Hiring company and site
Employer or platform owner	AI agent, with a named human owner	Internal system or partner API

How to open the conversation: “Passwords, contractor onboarding and recovery calls are where most workforce incidents start. Could we map one of those journeys and test whether wallet-based proof can sit alongside your current identity tools to make it faster and safer?”

Full use-case library (11 use cases)

Use case	What it does	Friction today	Start	Family
Passwordless Employee Login	Phishing-resistant sign-in with the wallet	Passwords are reused and phished	**Lead**	B
Contractor Onboarding & Time-Bound Access	Access that ends when the contract ends	Onboarding takes days of paperwork	**Lead**	A
Instant Offboarding & Revocation	Cut access everywhere, fast	Leavers keep access in forgotten systems	**Explore**	B
Converged Physical & Digital Access	One credential for doors and apps	Badge systems and IT access are separate	**Explore**	D
Service Desk & Recovery Protection	Close the recovery loophole	Callers talk agents into resets	**Lead**	C
AI Agent Authorization	A human owner behind every agent	Agents run on shared service accounts	**Emerging**	M
Privileged & Vendor Access Governance	Short, approved, recorded sessions	Standing admin rights stay on	**Explore**	B
Stale Entitlement Cleanup	Remove access nobody uses	Access reviews are slow and rubber-stamped	**Explore**	J
One Identity Every System	The same proof across apps, doors and partners	Each system keeps its own user record	**Explore**	B
Insider & Anomaly Detection	Spot odd access with strong signals	Logs show an account, not the person	**Emerging**	J
Qualification and safety-training checks	Training and licence credentials checked before role or site access	Certificates are scanned, copied and expire unnoticed	**Lead**	E

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Fewer password-related incidents and help-desk resets	• Time to onboard an employee or contractor
• Faster, safer contractor and vendor onboarding	• Password-reset and recovery tickets
• Fewer forgotten accounts after people leave	• Time to remove access after exit
• One audit trail across doors, applications and partners	• Orphaned or stale accounts found in reviews
• A named human owner behind every agent	• Service-desk social-engineering attempts (baseline first)
• A base the partner can add to its existing identity or managed-security offer	• Access-review effort in hours
	• Agents with a named owner and expiry

12. Loyalty programmes

Protect the points, keep the member experience easy

The business problem

Points and miles are a form of currency. Fake accounts farm sign-up bonuses, reused passwords open real accounts, and stolen points can be drained in minutes. Call centres are targeted, partner networks see members as unknown, and new member AI agents look much like bots. Programmes want less fraud without more friction.

Priority use cases

Use case	How iDen2 could fit
Enrolment and fake-account prevention	Bind each member to one verified identity before welcome bonuses are paid.
Passwordless member login	Offer wallet-based sign-in as an option next to the existing login.
Redemption authorisation	Ask for a wallet approval before high-value redemptions and transfers.
Call-centre verification	Replace quiz questions with a wallet check during the call.
Partner network verification	Let partners accept a member's proof of status without seeing the full account.
Member AI agents	Explore signed, limited authority for agents that spend points for a member.

Partner discovery question: Where do you lose points, money or member trust today: at sign-up, at sign-in, at redemption, on the phone, or at a partner?

Pro Tip: Members must opt in, and they must still be able to sign in without the wallet. Do not tell a programme that fraud will fall by a stated figure. Linking a member to a verified identity has privacy and data-law implications that differ by country. Treat points-as-currency rules and any digital-asset angle as needing legal review.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Loyalty programme or a government ID source	Member	Programme, partner brand or call centre
Programme	Member's tier or status	Partner hotel, airline, retailer or bank
Member	Member's AI agent, with spend limits and expiry	Programme booking or redemption system

How to open the conversation: “Points are worth money, so they attract fraud. Could we map one journey, such as redemption or the call centre, where stolen accounts or fake sign-ups cost you today, and test whether a wallet check helps without making honest members work harder?”

Full use-case library (10 use cases)

Use case	What it does	Friction today	Start	Family
Enrollment & Sybil Prevention	One person, one account	Fake accounts farm welcome bonuses	**Explore**	A
Passwordless Member Login	Sign in with a face, not a password	Reused passwords open accounts	**Lead**	B
Redemption Authorization	Protect high-value redemptions	Stolen accounts drain points in minutes	**Lead**	B
Bonus & Promotion Abuse Prevention	Promotions reach members, not farms	Promo codes are shared or farmed	**Explore**	B
Points Transfer & Gifting Controls	Safe transfers between people	Transfers are used to cash out stolen points	**Explore**	B
Partner Network Verification	Trust across brands and partners	Partners see a member as an unknown	**Explore**	H
Call-Center & Concierge Verification	Verify the caller without a quiz	Agents ask personal questions answered by breaches	**Lead**	C
AI Shopping & Travel Agent Authorization	Let members' agents spend points safely	Bots and member agents look alike	**Emerging**	M
Dormant Account Reactivation	Wake sleeping accounts safely	Inactive accounts hold points and are easy targets	**Explore**	B
Breach Containment	Limit the damage after a leak	Leaked passwords force mass resets	**Explore**	J

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Fewer fake accounts and less bonus abuse	• Fake or duplicate account rate (baseline first)
• Fewer account takeovers and drained balances	• Account-takeover cases and points lost
• Less friction at sign-in and redemption	• High-value redemption completion rate
• Shorter, safer call-centre verification	• Call verification time
• Stronger partner trust with less data shared	• Cost of promotion abuse
• Lower cost of mass password resets after a leak	• Share of members using wallet sign-in
	• Partner acceptance rate

13. Supply chain & logistics

Verified companies, people and goods from factory to customer

The business problem

Supply chains pass goods, money and paperwork between many companies that do not share a system. Suppliers are onboarded with weeks of document chasing, spoofed emails change bank details, certificates are scanned and copied, and cargo theft uses fake carriers and drivers. When a recall happens, teams hunt through records for the affected lots.

Priority use cases

Use case	How iDen2 could fit
Supplier onboarding and verification	Verify a company once and let buyers reuse the proof, with credentials issued by a registry or by the buyer.
Vendor payment and bank-change protection	Require a signed proof from the supplier before bank details change.
Parts and component provenance	Attach signed claims from the maker to parts, batches or certificates.
Chain of custody	Record each handover with signed events between known parties.
Carrier and driver identity	Check the company, driver and vehicle credentials at pickup.
Procurement agents	Explore signed limits for agents that request quotes or draft purchase orders.

Partner discovery question: Where in your supplier, payment, shipping or recall process do you currently trust a PDF, an email or a phone call that could be faked?

Pro Tip: A signed claim only proves who made the claim. It does not prove a part is genuine or a shipment is safe. Provenance needs sensors, scans or inspections at the physical edge, and every party in the chain must take part for the benefit to appear. Customs and product-authentication use cases depend on the authorities and brands involved and are early-stage.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Company registry, trade body or the buying company	Supplier	Buyer's procurement and finance teams
Manufacturer	Part, batch or certificate	Assembler, customs or customer
Carrier company	Driver and vehicle	Warehouse, port or shipper

How to open the conversation: “Supplier onboarding, bank-detail changes and shipment paperwork all rely on documents anyone can copy. Could we map one of those flows and test whether signed, checkable proof improves speed or cuts losses?”

Full use-case library (10 use cases)

Use case	What it does	Friction today	Start	Family
Supplier Onboarding & Verification	Verify the company once, reuse the proof	Onboarding takes weeks of document chasing	**Lead**	H
Vendor Payment & Bank-Change Protection	No wallet proof, no bank change	Spoofed emails change bank details	**Lead**	H
Parts & Component Provenance	Trace parts back to the maker	Certificates are scanned and copied	**Explore**	I
Chain of Custody & Cargo Transfer	Prove each handover	Handovers rely on signatures and photos	**Explore**	I
Carrier & Driver Identity	Right driver, right truck, right load	Cargo theft uses fake carriers and drivers	**Explore**	H
Customs & Trade Compliance	Share proof, not piles of paper	Declarations rely on documents that can be altered	**Emerging**	I
Factory & Facility Access	Verified people on site	Visitors and contractors get shared badges	**Explore**	D
Product Authentication	Let customers check what they bought	Fake goods look identical on the shelf	**Emerging**	I
Recall & Traceability	Find affected lots in hours, not weeks	Recalls start with a hunt through records	**Explore**	I
AI Agent Authorization	Procurement agents with a human behind them	Agents send orders and drafts with no proof of authority	**Emerging**	M

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Faster supplier onboarding with less document chasing	• Supplier onboarding lead time
• Fewer payment-diversion and fake-vendor losses	• Bank-change requests verified out of band (baseline first)
• Better proof of origin and handling	• Payment-diversion attempts and losses
• Quicker, narrower recalls	• Share of parts with signed provenance
• Safer pickups and site access	• Time to identify affected lots in a recall
• Clear records of what each procurement agent may do	• Pickup exceptions and cargo-theft incidents
	• Customs documentation delays

14. Travel & hospitality

One trusted traveller identity from booking to boarding to the hotel room

The business problem

A trip involves a booking site, an airline, an airport, border control, a hotel and often a loyalty programme. Each one checks the traveller again, with separate documents and queues. Fake bookings, account takeover and call-centre fraud add cost, and travel agents acting for people are an early AI use case.

Priority use cases

Use case	How iDen2 could fit
Booking and payment trust	Confirm the traveller behind a booking before high-risk changes or refunds.
Airport and boarding	Let a traveller present a verified identity credential at supported checkpoints, subject to the authority's rules.
Hotel check-in and room access	Use a pre-verified credential for check-in and, where integrated, for room access.
Crew and staff credentialing	Issue role, licence and security-clearance credentials for crew and hospitality staff.
Group and family delegation	Let one traveller act for others with limited, clear authority.
Travel agents	Explore signed limits on what an AI travel agent may book and spend.

Partner discovery question: Where in the journey, from booking to the room, does the traveller get asked to prove the same thing again, and where does fraud enter?

Pro Tip: Airport and border use cases belong to the authorities, not the airline or hotel. Do not promise biometric boarding or border acceptance. Hotel and airline use cases need agreements across several parties before a traveller sees any benefit. Start with hotel, loyalty and contact-centre cases, which one company can control.

Who issues, who holds, who verifies

Issuer	Holder	Verifier
Government ID source or national digital ID	Traveller	Airline, hotel or booking platform
Airline or hotel group	Traveller (booking, status or loyalty)	Partner airline, hotel or service desk
Airline, hotel or licensing body	Crew or staff member	Employer, airport or property

How to open the conversation: “Travellers show the same documents at booking, at the airport and at the hotel. Could we map one part of that journey, such as hotel check-in or loyalty protection, and test whether a pre-verified credential saves time or cuts fraud?”

Full use-case library (12 use cases)

Use case	What it does	Friction today	Start	Family
Booking & payment trust	Confirm the person behind a booking, change or refund	Fake bookings and chargebacks; weak checks on changes	**Explore**	B
Airport security & boarding	Verified identity credential at supported checkpoints	Documents are checked repeatedly by different parties	**Emerging**	A
Crew & staff credentialing	Licence, training and clearance credentials for crew and staff	Paper records and manual checks across employers	**Explore**	E
Hotel check-in & room access	Pre-verified guest credential for check-in and room entry	Front-desk queues and repeated document capture	**Lead**	D
Loyalty account protection	Wallet approval before points redemption or changes	Stolen accounts and drained balances	**Lead**	B
Contact-centre verification	Wallet check during the call before changes or refunds	Agents ask quiz questions answered by breached data	**Lead**	C
Border & visa eligibility	Prove a visa or eligibility status without sharing the full file	Manual checks at the airline desk and the border	**Emerging**	K
Age & eligibility proofs	Prove age or entitlement with the least data	Full documents shown for a single fact	**Explore**	K
Group, family & travel-party delegation	One traveller acts for children, family or a group within set limits	Paper letters and repeated proof for each person	**Explore**	F
Partner & concierge network trust	Partners accept a guest's proof of status without a full account	Each partner treats a guest as unknown	**Explore**	H
AI travel agents	Signed limits on booking and spend by an agent	No way to tell a guest's agent from a bot	**Emerging**	M
Digital signing of terms and waivers	Sign terms, waivers and consent in the wallet	Paper forms at desks and tour counters	**Explore**	G

Business value to test, and measures for a business case

Business value to test	Measures for a business case
• Shorter queues at check-in and boarding where authorities allow it	• Check-in time per guest
• Fewer fake bookings, takeovers and refund abuse	• Booking fraud and chargeback cases (baseline first)
• Better protection for loyalty balances	• Loyalty account-takeover cases
• Less repeated capture of the same documents	• Contact-centre handling time
• Clear delegation for families, groups and agents	• Share of guests using a pre-verified credential
• A shared trust layer across airline, hotel and partners	• Crew credential check time
	• Refund and change disputes

15. AI trust brief: Who authorised the agent?

AI agents are moving from answering questions to using tools, accessing systems, and initiating actions. That creates a trust question: how can a receiving organisation establish which agent is making a request, who it represents, what it is permitted to do and whether that authority is still valid?

Four questions a business should ask

1. **Identity:** Can the receiving system distinguish the agent from the human or organisation it represents?
2. **Authority:** Is there verifiable evidence that the principal authorised the agent to perform this type of action?
3. **Scope and duration:** Is the action within the limits of the delegation, and has the mandate expired or been revoked?
4. **Accountability:** Can the organisation preserve evidence of the mandate, policy decision, and action for audit and dispute handling?

Illustrative scenarios

Sector	Example agent	Trust question
Banking	Agent prepares a loan application or payment request	Who authorised it, and what steps still require customer or bank approval?
Telco	Agent requests service changes or provisioning	Which account or organisation does it represent, and what can it change?
Education	Agent submits qualifications or training evidence, or an advising agent acts for a student	Can the receiving institution verify the credentials and their source?
E-commerce	Agent buys goods or negotiates with a seller	What purchasing scope, value limit, and expiry apply?
Oil & gas	Agent requests supplier quotes or prepares purchase orders	Which supplier list, budget, and approval rules constrain it?
Insurance	Agent submits a claim or gathers underwriting evidence	What is it authorised to submit, and which decisions require human review?
Government	Agent helps a citizen or caseworker prepare an application	Whose authority does it carry, and which steps stay with a human official?
Healthcare	Agent drafts documentation or prior-authorisation requests	Which clinician or patient authorised it, and what health data may it touch?
NGOs	Case-support tool or chatbot touches beneficiary data	What may it see, and how is access to sensitive records limited?
Workforce	Agent runs on a service account inside company systems	Which human owns it, and what scope and expiry apply?
Loyalty	Member's agent redeems points or books rewards	What spend limit and expiry did the member set, and can the programme tell it from a bot?
Supply chain	Procurement agent sends orders or drafts	Which budget, supplier list and approval rules apply?
Travel & hospitality	Agent books travel or hotel services	Can the service provider verify the principal, the delegation, and the permitted spend?

Where iDen2 may fit

- Establishing a verifiable relationship between an agent and a human or organisational principal.
- Representing delegation through a signed mandate with defined scope and validity, if supported by the selected product configuration.
- Checking the mandate and its status at the point of use, subject to system connectivity and the revocation model.
- Providing cryptographic evidence and audit data to complement the customer's IAM, API security, monitoring and governance systems.

The responsible message

iDen2 should be positioned as a potential identity, trust, and delegation layer, not a complete AI security solution. Agent permissions, sandboxing, prompt-injection defence, model evaluation, transaction controls, human oversight and incident response remain separate requirements. Agent Proof of Control is in development; do not describe it as generally available.

AI discovery questions

- Which agents can currently access production systems or initiate external transactions?
- How is each agent associated with a person, team or legal entity?
- How are permissions scoped, approved, time-limited and revoked?
- What evidence is available if an agent's action is challenged?
- Which high-value or high-risk action could be piloted with a narrow scope and human approval?

Pilot blueprint: from interest to evidence

A pilot should prove a specific workflow outcome, not attempt to demonstrate the entire platform.

Pilot stages

1. Select one use case, one customer process and one business owner.
2. Map the current process, participants, data flows, trust assumptions, and control points.
3. Confirm the issuer, credential contents, holder/presentation method, verifier, and status-check model.
4. Confirm legal basis, privacy, data residency, retention, security, and regulatory review with the customer.
5. Agree integration scope, test environment, test data, responsibilities, and support arrangements.
6. Define baseline metrics and success criteria before testing.
7. Run a limited pilot, document exceptions, and compare outcomes against the baseline.
8. Decide whether to stop, refine or expand into production; agree on commercial terms and operating ownership.

Suggested metrics by use case

Use case family	Potential measures
Onboarding and reusable verification	Time to complete; cost per completed case; manual-review rate; abandonment; duplicate-record rate
Login and payment protection	Account-takeover cases; reset tickets; step-up completion rate; false rejections; drained-balance losses
Caller verification	Call handling time; failed verifications; social-engineering attempts caught (baseline first)
Physical and site access	Time to grant and remove access; badge exceptions; shared-credential incidents
Qualifications and licences	Time per check; follow-up rate; expired-credential exceptions; manual audit hours
Delegation and guardians	Time to set up authority; paper forms removed; disputes about who could act
Digital signing	Time to signature; completion rate; failed or disputed signatures; audit completeness
Supplier and partner checks	Onboarding lead time; bank-change requests verified; fake-vendor attempts
Provenance and custody	Share of items with signed records; time to trace affected lots; handover disputes
Minimum-disclosure proofs	Time to verify eligibility; data fields collected per person; false acceptance and rejection
Offline and field	Share of checks completed offline; sync errors; time to enrol in the field
AI-agent delegation	Mandate validation success; out-of-scope actions blocked; revocation response; audit evidence completeness

Pro Tip: Use customer baseline data and pilot measurements to establish savings. Do not publish percentages, fraud-reduction claims or payback periods unless they are supported by reliable evidence and approved for external use.

Suggested first pilot by sector

These are starting suggestions for the first discovery workshop. They are drawn from the Lead-tagged use cases and need customer validation.

Sector	Suggested first pilot	Main caution
Banking	Wallet check before payee, address or device changes, or in the call centre	Does not replace KYC, AML or fraud controls
Telecom	Wallet approval before SIM change or port-out	Does not replace SIM-registration rules
Education	Digital diploma and transcript for alumni, verified by employers	Employer acceptance must be agreed
E-commerce	Verified age or eligibility proof at checkout, or protected account sign-in	Marketplace-wide acceptance takes time
Oil & gas	Contractor competency and safety-training credentials at site entry	Worker privacy and the site's access system
Insurance	Verified policyholder at claim or policy change	Does not replace fraud investigation
Government	One programme where one agency's verified fact is accepted by another	Procurement route and national ID scheme
Healthcare	Patient or caller verification at registration and in the contact centre	Health-privacy law; no compliance claims
NGOs	Field worker and volunteer credentials, with a small, low-risk beneficiary pilot later	Protection and consent review; funding source
Workforce	Passwordless login or recovery protection for one user group	Works with the existing identity provider
Loyalty	Wallet approval for high-value redemptions, or call-centre verification	Members must be able to opt out
Supply chain	Supplier onboarding and bank-change verification for one buyer	Needs suppliers to hold a wallet
Travel & hospitality	Hotel check-in credential and loyalty account protection	Airport and border pilots belong to the authorities

Positioning, objections, and guardrails

Customer objection	Suggested response
“We already have IAM / SSO.”	“Those systems remain important. The question is whether you also need portable credentials or verifiable evidence across organisations that do not share the same identity system.”
“We already use an identity-proofing provider.”	“We should assess how iDen2 would complement that provider, perhaps for issuing, presenting or verifying reusable credentials, rather than assume replacement is necessary.”
“Why not use a database?”	“A database may be the right choice for some workflows. A credential-based approach is worth evaluating where a holder needs to present verifiable evidence across systems or organisations.”
“Does this eliminate fraud?”	“No single control eliminates fraud. We would define the specific threat and test whether verifiable credentials, status checks and stronger evidence improve the workflow alongside existing controls.”
“Does it guarantee compliance?”	“No. Compliance depends on the jurisdiction, use case, issuer, controls, integration, and the customer's obligations. We would involve legal and compliance teams early to design for compliance.”
“Will every organisation accept the credential?”	“No. Acceptance requires compatible technology, trust in the issuer, appropriate policies, and a legal and operational basis. The solution is built with interoperability in mind, and value grows as more organisations join.”
“Why do we need this for AI?”	“As agents act across systems, organisations may need better evidence of identity and delegated authority. The relevant use case should be scoped alongside existing IAM and AI security controls.”
“Is this blockchain?”	“The conversation should start with the business outcome and trust model. We can explain the architecture and any ledger dependencies accurately when they matter to your requirements.”
“Will it replace our signing provider?”	“That depends on the signing method, legal requirements and integration. We should identify whether iDen2 can complement or support the required signing workflow and confirm the applicable evidence.”
“Who is the issuer, and why would anyone trust it?”	“Trust comes from the issuer, not from iDen2. Each verifier decides which issuers it accepts. Part of discovery is to name the issuer that your verifiers already trust.”
“What about privacy and biometrics?”	“Privacy rules differ by country. We would agree what data is needed, where it is held, and whether biometrics are used at all, with your privacy team and local counsel.”
“What if the person loses their phone?”	“Recovery is a design decision for each use case. We would confirm the options the product supports and agree a policy with you before any pilot.”
“Can it work offline?”	“Some checks may work offline, depending on the product configuration and how status is checked. We will confirm the exact behaviour for your use case before promising it.”
“Who already uses this at scale?”	“We would rather show you a bounded pilot with your own numbers than quote adoption claims. We can share what iDen2 has approved for external use.”
“Is this a replacement for a national ID?”	“No. iDen2 does not issue or replace national identity. It lets organisations issue and check credentials, and can work with a national scheme where one exists.”

Claims that need product/legal approval before use

- “Compliant with” any named national law, regulation or certification, including HIPAA, GDPR, eIDAS or any health, privacy or payments rule.
- “Legally binding” or “qualified electronic signature” in a specific jurisdiction.
- “Eliminates fraud,” “prevents deepfakes,” “stops all account takeover,” or “guarantees identity.”

- “Works offline,” “supports all wallets,” “integrates with any system,” or “instant revocation” without confirming the exact product behaviour.
- Specific performance, savings, speed, deployment time, uptime, scale, or customer adoption figures, including third-party statistics.
- Security certifications or audits (for example SOC 2, ISO 27001 or a presentation-attack-detection level) unless iDen2 has confirmed them in writing.
- “Deployed”, “in production” or “proven at national scale”, and any named government or customer deployment, unless approved for external use.
- Post-quantum security as a current feature, or “certified” against any named standard or framework.
- That a feature on the roadmap or in development (Intelligent Wallet, Agentic Wallet, Agent Proof of Control) is available today.

Country-specific localisation checklist

Use the following as a discovery checklist, not as a statement of country-specific legal requirements. Confirm current rules with local counsel and the customer's compliance team.

Area	Questions to resolve
Identity & KYC	Which official identity sources are accepted? What proofing and ongoing due diligence are required?
Privacy & data	What personal data is necessary? Where may it be stored or processed? What cross-border transfers and retention rules apply?
E-signatures	Which signature types are recognised for this document and transaction? Are there witnessing, notarisation, qualified trust-service, or local-provider requirements?
Financial services	What do the regulator and institution require for onboarding, AML/CFT, sanctions, recordkeeping, and audit?
Telecom	What subscriber-registration, SIM, account recovery, and network-security requirements apply?
Employment / oil & gas	Which worker qualifications, safety training, site access and contractor checks are required? What data is sensitive? Do labour or works-council rules limit biometrics or monitoring?
Insurance	What licensing, claims-handling, anti-fraud and data-sharing rules apply to identity and evidence?
Healthcare	What health-privacy, consent, e-prescribing and clinician-licensing rules apply? Who may see which records?
Government procurement	Are local hosting, certification, sovereign control, approved vendors, or local delivery partners required?
Humanitarian and protection	What protection, consent and safeguarding rules apply? Who may hold beneficiary data, and where? What do donors and host governments require?
Consumer programmes	Is opt-in consent needed to link members to a verified identity? What rules cover points, gifts and transfers?
Trade and logistics	Which customs, trade-document and dangerous-goods rules apply? Which authorities accept digital records?
Travel and border	Which authorities control airport, border and visa checks? Which of those checks may use a digital credential?
AI governance	What rules or internal policies apply to AI agents acting for people? Who is accountable for an agent's action?
Language & accessibility	Is English or other language interface and support needed? What accessibility requirements apply?
Trust ecosystem	Who are the trusted issuers? Which verifiers will accept the credential? How are status and revocation checked?
Deployment	Cloud, private cloud, or on-premises? What availability, disaster recovery, and support commitments are required?

Regional sales principle

Pro Tip: Keep the product claims and technical description consistent. Adapt the problem statement, examples, language, deployment model, regulatory analysis, procurement path and partner offer to each country and customer.

Partner and account planning worksheet

Duplicate this page for each partner and each priority customer.

Field	Working notes
Country/market	
Organisation/business unit	
Partner's core products and customer access	
Target sector/customer	
Customer business sponsor / technical owner	
Problem / current workflow	
Use-case family (A to M) and tag (Lead / Explore / Emerging)	
Issuer/evidence source	
Holder/presentation channel	
Verifier / relying system	
Existing identity provider, signing and access systems	
Potential iDen2 capability	
Integration/security dependencies	
Regulatory / privacy questions	
Business baseline and success measures	
Competitors / incumbent systems	
Pilot scope/exclusions	
Commercial model/decision path	
Next action/owner/date	

Initial use-case prioritisation

Score each candidate 1 to 5 against customer pain, repeatability across accounts, issuer availability, integration feasibility, partner advantage, measurable value, regulatory clarity and AI relevance. Prioritise use cases with clear pain, a credible issuer, an identified buyer and a bounded pilot, not simply the most futuristic use case.

Candidate use case	Initial view	Why / next validation
Caller and contact-centre verification (C)	Strong candidate	One organisation controls it; the pain is easy to measure. Validate the current call volume and fraud baseline.
Login, step-up and payment protection (B)	Strong candidate	Common across banking, telecom, loyalty and workforce. Validate the integration with the existing sign-in.
Business/supplier credential verification (H)	Strong candidate	Cross-sector relevance; identify trusted sources and required attributes.
Employment/contractor credential verification (A, E)	Strong candidate	Relevant to oil & gas, workforce and supply chain; validate worker privacy and the issuer model.
Education and professional credentials (E)	Strong candidate	Clear issuer-holder-verifier model; map institutions and employer acceptance.
Physical and site access (D)	Good candidate	Works where the customer controls the door or site. Validate the access-control integration.
Financial onboarding / reusable KYC (A)	High value, more regulated	Validate compliance acceptance, identity sources, and bank integration.
Minimum-disclosure and eligibility proofs (K)	Good candidate	Easy to explain. Validate who issues the attribute and who accepts it.
Digital signing (G)	Useful adjacent play	Confirm signature type, jurisdictional validity, and integration fit.
Delegation and guardians (F)	Potentially valuable	Strong user need; confirm legal basis for acting on behalf of others.
Telecom subscriber credential issuance (A)	Potentially valuable	Confirm who issues what, legal requirements, and existing national identity integration.
Provenance, custody and traceability (I)	Explore	Needs several parties and physical-world checks; start inside one company or one lane.
Offline and field verification (L)	Explore	Confirm exactly what works offline in the product before scoping.
Audit trail and compliance evidence (J)	Supporting capability	Position as a benefit of other use cases rather than a first sale.
AI-agent delegation (M)	Strategic emerging play	Start with a narrow workflow, mandate model, transaction limits, and human approval.

Quick-reference: what every partner should remember

The one-line story

iDen2 helps organisations issue, present and verify trusted digital credentials, and is developing trust capabilities for delegated actions by AI agents.

The five rules

1. Lead with a business problem, not technical standards.
2. Identify the trusted issuer and the evidence behind the credential.
3. Show how iDen2 complements the partner's existing solution and the customer's existing controls.
4. Prove value through a bounded workflow and agreed metrics.
5. Be precise about product capability, legal acceptance, security, and regional requirements.

The next step

Select one priority partner, one sector, and one workflow. Run a discovery workshop, map the issuer-holder-verifier chain, agree the current baseline and design a limited pilot. Use the learning to refine the partner pitch before scaling to additional accounts.

About this version (v3.0)

What changed from v2.0

- Sector guides grew from 8 to 13. New: NGOs & humanitarian, Workforce & enterprise access, Loyalty programmes, Supply chain & logistics, Travel & hospitality.
- Every sector now has a full use-case library, 152 entries in total, each tagged Lead, Explore or Emerging and linked to one of 13 use-case families.
- New: contents page, product maturity guide, use-case map and matrix, first-pilot suggestions by sector, and a fuller metrics table.
- Objections, claims-needing-approval, localisation checklist, AI scenarios and prioritisation were extended to cover all 13 sectors.
- The AI trust brief is now section 15 (it was section 10 in v0.2). Section numbers 10 to 14 now hold the five new sectors.
- Government was rewritten in neutral wording with no certification claims. Healthcare no longer uses “HIPAA-grade” or a named liveness level.
- Statistics from the sector decks are not included, because most are illustrative or unsourced. Add a figure only once iDen2 has a source it can defend.