Digidentity

A New Perspective On Employee Risk:

OBO

('On Behalf Of')

How to Protect the Business in the Moments That Matter

Brought to you by
Digidentity** and **Customer Futures

Executive Summary

Every organisation faces a deceptively simple but critical question: **What happens when an employee acts on behalf of the business?**

In today's digital, global environment, that question is harder to answer than ever. Hybrid working, automated workflows and GenAI systems have blurred the lines of authority. People change roles, delegate responsibilities, and act across departments or even between organisations. Yet most organisations still rely on static records to prove who's authorised to do what.

Identity and Access Management (IAM) platforms keep internal systems secure. But they weren't built to prove representation or authority *outside* the company walls. When an employee signs a contract, approves a supplier, or files a regulatory report, the real question isn't '*who logged in?*', it's '*who were they representing?*' and *'were they still authorised to act?'*

This paper introduces a new layer of trust for businesses: **On Behalf Of (OBO)**.

OBO turns internal access controls into verifiable, portable, auditable authority, and means employees can now prove they are genuinely allowed to act for their company. Not just *who* they are, but *what* they're allowed to do, right now.

Is OBO for you?

This paper is for organisations where trust, authority and accountability matter. Particularly for Legal and Compliance leaders, HR and Operations teams, IT and IAM specialists, and senior executives responsible for governance and risk.

And although the principles behind OBO apply worldwide, this paper highlights the momentum building in Europe and the UK. New frameworks including eIDAS 2.0, the upcoming Business Wallet Regulation, and the UK's DIATF are reshaping how organisations must prove authority.

These market shifts are making portable, verifiable delegation and representation not only possible, but increasingly essential.

When the Signature Outlasts the Role

It happens more often than anyone admits.

Imagine Elena, a senior operations manager, leaves her company after six productive years. Her email account is closed, her laptop returned, and her HR record archived. A few weeks later, a supplier sends through a minor contract amendment, a routine renewal that had been discussed before she left.

The workflow tool still lists Elena as the authorised approver, so the request lands in the shared team inbox. A colleague, assuming Elena is still responsible for that supplier, clicks “approve” on her behalf. The platform records the action under Elena’s name, even though she no longer works for the company.

At first, nobody notices. The amendment sits quietly in the files until the annual audit, when the legal team discovers the signature date doesn’t match Elena’s employment record. The supplier’s lawyers insist the contract is valid. There’s no verifiable evidence showing she wasn’t authorised at that moment.

The problem is that this wasn’t fraud. It was just another frictionless failure. The kind that slips through the gaps when our systems move slower than our people.

Every business has its own version of Elena’s story. A temporary approver who keeps access too long. A regional director who signs on behalf of a partner without updated authority. A new manager who inherits the wrong permissions.

Authority, it turns out, changes faster than most systems can keep up. **And that’s the hidden risk:** the moment when trust is assumed, but no longer proven.

Employees constantly change roles, cover absences, act in cross-functional projects, and represent the company externally. Yet most businesses still manage authority with spreadsheets, emails, and trust. When the question is *“Who signed this, and were they allowed to?”* the answer is rarely verifiable. And every audit trail begins too late.

OBO now moves trust to the moment of action. To when it matters.

The Illusion of Control

On paper, employee identity looks tidy. Everyone has a staff number, an email address, and a set of permissions. HR systems record job titles, and IAM platforms log every login.

But in practice, none of it stays still. People rotate between projects, fill in for colleagues, take on new responsibilities, or move on entirely. Contractors act for the company one week and for a supplier the next. And automated processes complete actions "on behalf of" someone who's already left.

And every industry has its own version of this illusion.

In financial services, analysts retain approval rights for portfolios they no longer manage. In healthcare, clinicians use shared credentials long after a rota change. In government, temporary staff access citizen records beyond their assignment.

Each case shows the same pattern: systems assume continuity, while reality keeps changing. It's comforting to think that the audit trail covers every risk. But most trails stop at the moment of login. They prove *who entered the system*, not *why they acted* or *for whom*.

This illusion of control is fine… until the day of audit, dispute, or investigation. Then it collapses into a scramble to reconstruct authority after the fact.

> *"IAM tells you who can log in.*
> *OBO proves who's allowed to act."*

Why IAM Isn't Enough

For most organisations, the Identity and Access Management (IAM) system is the backbone of digital security. It governs who can log in, what they can see, and how long their permissions last. Mature IAM platforms automate onboarding, link to HR systems, and even trigger de-provisioning the moment someone leaves.

And inside the organisation, it works brilliantly. But authority doesn't stop at the company front door. Because when employees act *on behalf of* the company - signing documents, approving transactions, submitting reports - their digital footprint moves beyond IAM's reach.

IAM records access events. It rarely proves *representation.* Even the most advanced IAM and Governance tools face four blind spots:

1. **External representation**: IAM governs access *inside* systems, not authority *across* organisations.
2. **Temporary delegation**: Many systems don't model time-bound authority: *"Approve for two weeks while I'm away."*
3. **Context and intent**: Logs show actions, not the organisational context behind them.
4. **Portability**: Credentials can't travel securely between systems or companies.

Consider a partner portal that tracks a project manager's logins. It confirms she accessed the system, but not whether she's still authorised to approve for her company, or if she's now in a different role entirely.

Yes, some IAM systems model time-bound access internally, but only when tightly integrated with HR and lifecycle data. In practice, those integrations are often complex and costly to maintain. OBO extends that capability 'outward', linking internal lifecycle events (a temporary job move) to *external* proof of authority.

Of course, IAM remains essential. It manages internal access and auditability. But **OBO extends IAM's assurance beyond the business,** linking access to verifiable authority, and ensuring that when someone acts, it's clear who they represent and why.

"IAM governs internal access.
OBO adds external and time-bound context."

The Regulatory Shift Making OBO Inevitable

OBO is not emerging in a vacuum. Several major regulatory developments in Europe and the UK are creating a clear need for portable, verifiable authority within organisations and across borders.

eIDAS 2.0 (2024)
The updated 'eIDAS2 framework' introduces new formal mechanisms for expressing representation, delegation and mandate management. It strengthens the legal role of QES and eSeals, and establishes standardised ways for organisations to issue "Power of Representation" attestations to employees, the foundation of cross-border business identity, and the shift towards OBO credentials more generally.

Business Wallet Regulation (EU)
The upcoming 'Business Wallet Regulation' builds on eIDAS 2.0 by defining how companies and employees will hold and present *business credentials* - including roles, mandates and signing authority - inside *trusted digital wallets*. This creates a legal and technical pathway for OBO credentials to be recognised across Member States.

UK DIATF (the 'Digital Identity and Attributes Trust Framework')
And in the UK, the DIATF establishes 'trust lists' and 'assurance models' for digital identities, attributes and organisational credentials. It provides a regulated foundation for verifying who someone is and who they represent, enabling OBO in regulated sectors.

Together, these developments make it possible, and increasingly necessary, for organisations to issue, manage and verify *live, portable authority*. OBO is the operational model that brings these regulatory concepts to life.

But this begs a new question: how will external parties verify OBO credentials in practice?

QES already provides universal legal acceptance under eIDAS and can be validated by any standard signing tool. Yes, new Verifiable Credentials (VCs) add portability, revocation and real-time authority, but they also now require the 'verifier' to have the ability to check the credential and trust the issuer.

In reality, organisations won't need a fully deployed ecosystem or real-time 'VC verification' to benefit from OBO today. Much of the value comes from *post-transaction auditability*. Having a portable, tamper-proof record that shows *who acted, for which organisation, and with what authority at the time*. This mirrors the way QES works today in many regulated workflows.

The good news is that for those partners who don't yet have 'VC-native' verification, Digidentity can provide a verifier service that allows external parties to validate OBO credentials directly, without deploying wallet infrastructure. It means organisations can adopt OBO *now,* while preparing for wider ecosystem adoption.

And as new cross-border frameworks mature, including eIDAS 2.0, the Business Wallet Regulation, and the UK's DIATF, *the verification landscape will continue to standardise*. This creates the foundations for scalable, interoperable OBO flows, where authority can be recognised across all sorts of business networks, across different sectors and of course multiple jurisdictions.

Introducing OBO: 'On Behalf Of'

'On Behalf Of' (OBO) is a simple idea with far-reaching impacts. The ability to prove, in real time, who is authorised to act for an organisation, in what context, and for how long. At its core, OBO connects three moving parts that until now have lived in separate systems:

1. **The Organisation**: the entity being represented
2. **The Individual**: the person performing the action
3. **The Context**: what is being done, and under what authority

When those three are combined, they create an **OBO credential**. A verifiable proof that the person is authorised to act for that organisation, within that specific scope and timeframe. In practice, an OBO credential might:

- Accompany a Qualified Electronic Signature (QES) on a contract.
- Sit inside a digital wallet, ready to present to partners or regulators.
- Embed into workflow tools so automated approvals always carry proof of authority.

Unlike static job titles or role-based permissions, OBO credentials are 'live'. They can expire, be revoked, or change scope instantly. That means temporary delegation, cross-department projects, and external representation all remain auditable and up to date.

This point is key: OBO doesn't replace IAM or HR systems. Rather, it builds a bridge between them. It turns access into authority, and assumptions into evidence.

OBO credentials can take different forms, depending on the context and the level of assurance needed. For example:

- **Representation Credential:** Used when an employee acts on behalf of the organisation externally. For example, signing a government filing or representing the company in a joint venture.
- **Approval Credential:** This would be embedded in workflow tools to prove that a specific person was authorised to approve or release funds at the time of action.
- **Regulatory or Legal Credential:** Attached to a Qualified Electronic Signature (QES) or eSeal for high-assurance actions such as board minutes, compliance filings, or intergovernmental reporting.

Note that these OBO credentials can be expressed in a number of different ways, to meet the business's needs. It could be as an 'eSeal' embedded directly within existing signing, HR or workflow platforms. Or it could be stored in an employee's digital wallet, as a verifiable credential (VC).

"Authority now needs to be as portable and provable as identity."

The OBO Zones Framework

Not every action carries the same risk. A receptionist logging into an office system isn't the same as a director signing a regulatory filing. Yet both are treated through the same lens of identity and access.

The OBO Zones framework helps organisations map where authority becomes complex, and where traditional IAM stops providing assurance. Imagine three layers of organisational maturity:

1. Compliance: knowing who
This is where most IAM systems operate today. Identity checks, passwords, permissions. It's about individual authentication, making sure the right person logs in. It answers who, but not why.

2. Control: knowing what they can do
Here, authority spreads across *teams*. Employees approve, delegate and act across departments. Roles evolve faster than systems can update. The question shifts from *"who are you?"* to *"what are you authorised to do right now?"* This is where many organisations begin to lose visibility.

3. Continuity: knowing how trust travels
Beyond the enterprise perimeter, employees represent the business to customers, suppliers, and regulators. These moments require portable proof: verifiable across systems and time.

When you map the OBO zones in your business, you can see a ladder of digital authority. Where each step adds both value and risk. From simple compliance checks, through active control, to long-term continuity across organisational boundaries.

Zones	Focus	Key Question	Example
1. Compliance	Individual tasks inside departments	"Did we check who this person is?"	An employee badges into the office or logs into the HR system
2. Control	Multiple tasks across departments	"Is this person still authorised to act?"	A team lead approves spend or onboarding across teams
3. Continuity	Multiple roles across organisations	"Can we prove authority across time and partners?"	A director signs or represents the company to regulators

Understanding where your employees sit on that ladder - and how they move between zones - is the first step toward managing modern authority.

"OBO turns static roles into dynamic relationships of trust."

OBO in Practice: How Authority Really Moves

While the idea behind OBO is simple, the reality inside organisations is anything but. Every day, people act *on behalf of* their employer - signing, approving, submitting, or representing - without a clear, verifiable record of authority.

Here are some examples showing where trust can quietly break down.

External Interactions

A contracts manager signs a supplier renewal on an e-signature platform. Her identity is confirmed, but her authority isn't. The signature appears valid, yet no record links it to a current role. During a later dispute, the supplier insists the contract stands, but the business must scramble to prove otherwise.

Now with OBO: her signature carries a credential tied to her live role and department. If she moves or leaves, the credential automatically expires. The result is evidence that survives the handover, and proof that authority was valid at the time of action.

Temporary Interactions

A compliance officer steps in for a manager on leave, approving risk reports for two weeks. The temporary delegation is managed by email, and then quietly forgotten. Months later, during a review, they still hold access to restricted systems.

Now with OBO: temporary authority is issued as a time-bound credential that expires automatically. Everyone can see who is currently acting on whose behalf. No manual clean-up needed. And no silent drift of power.

Cross-Organisation Collaboration

A product lead is embedded into a joint venture with two partner firms. Each system recognises them as “external,” but neither side can verify they're genuinely authorised to approve on behalf of the other company. Work slows as every decision needs a human confirmation chain.

Now with OBO: both organisations issue credentials that can be verified in real time. The product lead now presents a single portable proof, recognised across domains, that travels with them as long as the collaboration lasts.

Across all three scenarios, the same pattern repeats: **authority is assumed until it fails.** OBO flips that pattern. It turns authority into a verifiable fact, ensuring that every action - internal or external, temporary or ongoing - *carries a live proof of legitimacy.*

> *"Most authority leaks happen between systems, not within them."*

Why This Matters (And Who Should Care)

Here's the thing. OBO touches every team that depends on trust, authority, and governance.

Below, we look at the people who stand to gain the most from new OBO flows across the business.

For Legal and Compliance Leaders

Legal teams must prove not just what was signed, but *who had the authority to sign it.* When something goes wrong, that distinction decides who carries the liability. OBO brings time-bound, verifiable proof of authority that stands up to scrutiny in court, in audit, or under regulatory review.

Instead of searching through emails and SharePoint folders, *the evidence travels with the signature itself.* Embedded, portable, and tamper-proof. It gives legal and compliance officers a higher standard of assurance, where they can now demonstrate, instantly, that the person acting was genuinely empowered to do so.

That clarity accelerates due diligence, reduces disputes, and turns compliance from a defensive exercise into a proactive safeguard.

For HR, Operations and Governance

As we've mentioned, company roles evolve faster than systems can keep up. With promotions, parental leave, project rotations, every personnel change alters who can legitimately approve, delegate, or represent the organisation. But most HR and operations systems treat authority as static.

OBO links delegation directly to the employee lifecycle. So when someone joins, moves, or leaves, their authority updates automatically. And temporary powers can expire when the authority is no longer required. Covering a colleague's absence becomes a controlled, auditable process instead of a chain of emails.

Technologies like 'IGA' and 'SCIM' do some of this already. Keeping identity data synchronised between HR and IT systems, and ensuring the right person has the right access. But those solutions are focussed on *internal* processes within the business. OBO builds on those foundations, issuing and revoking authority credentials that can now travel *beyond* internal systems.

Put another way, IGA *synchronises roles*, and OBO proves *representation.* OBO now creates a twin benefit: *continuity* for the organisation, and *protection* for the employee. No one can act beyond their role or mandate, and governance can finally move at the same speed as the work being carried out.

For IT and IAM Leaders

IAM already secures internal access and tracks activity with precision. But its design stops at the organisational boundary, where it wasn't built to confirm representation across partners, suppliers, or regulators.

OBO builds on IAM's foundation rather than replacing it. It uses existing identity signals, role data, and lifecycle events. *Adding a verifiable layer of authority that travels wherever the employee acts.*

For IT leaders, OBO means fewer manual role updates, cleaner audit logs, and stronger assurance for every external interaction. It connects IAM, HR and workflow tools into a single layer of trust. And because it's based on open standards like verifiable credentials, QES, and wallet technology, it scales naturally across systems.

OBO doesn't compete with IAM. It *extends* its reach into the real world beyond the front door.

For Executives and Risk Officers

Executives carry the responsibility for every decision made under their brand. Yet many of those decisions are delegated, distributed, or automated. It creates risk without visibility.

OBO delivers something new: **dynamic governance**. Real-time insights into who acted, on whose behalf, and with what authority. It replaces post-incident investigation with pre-emptive proof. It's new assurance that protects both the company and its people. Leaders can now delegate with confidence, knowing authority is controlled and verifiable. And when something goes wrong, the evidence chain is already in place.

OBO shifts governance from after-the-fact accountability to always-on assurance. A new foundation for trust in the digital economy.

"OBO isn't an IT upgrade
It's a new shared layer of accountability."

The OBO Stack: The Building Blocks Are Already Here

The good news is that OBO doesn't require a revolution in the company's infrastructure. **Most of what's needed already exists inside modern enterprises.** It simply needs to be connected. Think of it as four layers of trust that work together to transform identity into *authority*:

Layer	What it does	Typical tools today
QES & eSeals	Provide legally binding proof that an identified person or company executed an action.	Qualified trust services, digital signing platforms
Verifiable Credentials	Express who someone is authorised to represent and under what scope.	W3C VCs, organisational attestations
SCIM / IGA	Keep IAM and HR data synchronised as people change roles.	Lifecycle-management systems
Digital Wallets	Store and present credentials securely, under user control.	Enterprise or cloud wallets

When combined, these layers create a new kind of Staff Passport. A living proof of organisational authority that travels with the employee, yet remains governed by the business.

Imagine an approver signing a supplier contract:

- The signature of the individual is backed by QES (legal assurance)
- The Verifiable Credential confirms their level of authorisation
- The IGA system updates the credentials when they change teams
- Their wallet presents and stores that proof whenever needed

Together, these layers **turn static identity into dynamic assurance**. A continuous chain of evidence linking access, authority, and accountability. And because each layer already exists in mature enterprise stacks, adopting OBO isn't a leap of faith. It's a matter of orchestration.

> *"The future of digital trust doesn't require new technology.*
> *We just need to connect what we already have."*

The roadmap to Adopting OBO

As we've mentioned already, OBO isn't a 'rip-and-replace' project, it's more of an evolution of the systems you already trust. Most organisations can start small, prove value quickly, and build momentum from there.

Here's how you should think about adopting OBO:

Step 1 – Map where IAM stops
List the points where employees act on behalf of the company beyond internal systems. Digital signing, supplier approvals, partner logins, regulatory submissions. These are your highest-stakes "OBO gaps."

Step 2 – Prioritise high-impact zones
Begin where the risk/reward ratio is clearest: external signatures, cross-org approvals, or time-limited delegations. Choose one workflow and make authority verifiable from end to end.

Step 3 – Pilot OBO credentials
Issue credentials through existing wallets or signing platforms. Demonstrate how authority can be checked, revoked, or renewed without touching core IAM systems.

Step 4 – Extend across partners and regulators
Once internal users are comfortable, connect the assurance loop externally. Encourage suppliers and counterparties to verify actions rather than trust static records. Where external partners do not yet have native verification capabilities, Digidentity can provide hosted verifier solutions.

Step 5 – Bake OBO into governance
Incorporate verifiable authority into compliance, audit, and risk frameworks. Treat OBO credentials as evidence equal to signatures or access logs.

Each of these steps builds comfort and visibility, without ripping out existing IAM or HR infrastructure. And each phase adds visibility and reduces friction so that within months,

OBO becomes a quiet layer of confidence that can run underneath the business.

Conclusion: Protecting the Business in the Moments That Matter

The question *"Who really signed that document?"* used to be rhetorical. Now it can become a critical business risk.

As digital transformation accelerates, authority must become as verifiable and portable as digital identity itself. OBO can now provide that missing assurance - for legal teams, for compliance departments, for HR and for IAM system owners.

Proof that the right person acted, with the right authority, at the right time.

For organisations, it's a shift from static control to *dynamic trust.* For employees, it's protection from acting outside their mandate. And for auditors and regulators, it's finally business assurance and clarity over actions that can be proven at the right time.

OBO isn't a future vision. The building blocks exist today. The opportunity - and the responsibility - is to connect them now, before the next moment that matters arrives.

Digidentity and Customer Futures can help you get there. To design and execute that first step towards OBO. From mapping the risks and defining an OBO model for your business, through to running a live pilot with your existing stack.

If you'd like to explore an OBO pilot, or understand what this would look like in your organisation, please get in touch with **Digidentity** or **Customer Futures**.

About Digitdentity - www.digidentity.eu

Digidentity is a pioneer in the digital identity space. The platform has successfully verified over 25 million high-assurance identities, offering the convenience of reuse across multiple services. The platform is designed to make it easy for our customers to verify identities across multiple platforms and services, making it a one-stop shop for all verified identity needs.

We proudly serve as a trusted partner to governments, healthcare providers, and 175,000 corporate businesses, with verified identities from over 180 nationalities. Our commitment to security is evident in our inclusion on prestigious trust lists, including the UK's Digital Identity and Attributes Trust Framework (DIATF) and the Adobe Approved Trust list (AATL).

About Customer Futures - www.customerfutures.com

Customer Futures is a strategic advisory and thought leadership firm focused on the next generation of digital trust, identity, and customer experience. We help organisations understand and respond to the rise of Empowerment Tech; the new wave of digital wallets, verifiable credentials, and AI agents that put individuals back in control of their data.

Through research, advisory projects, and community programmes, we equip business leaders with the insight, language, and frameworks to navigate the critical and complex digital shifts around customer data. The Customer Futures newsletter and events network connect thousands of global executives, helping them anticipate change, shape new markets, and design trusted digital relationships for the decade ahead.