IDX

TRANSFORMING CONTRACTOR IDENTITY MANAGEMENT WITH ADIA

www.authid.ai | (516) 778-5639

IDX – Transforming Contractor Identity Management with ADIA

By: Erick Soto, authID Chief Product Officer

Contents

INTRODUCTION: SECURING THE CONTRACTOR BLINDSPOT

Contractors are essential to modern enterprises, yet they often remain an IAM blind spot introducing significant security risk if not managed properly. In fact, 61% of organizations experienced a third-party breach in the last year (a 49% YoY increase), and nearly 29% of all breaches involve third-party access. Traditional identity solutions struggle to give contractors unique, verified identities without cumbersome processes, leading to shared logins and manual workarounds. This not only violates security best practices (shared accounts cause a loss of accountability and are barred by compliance mandates) but also exposes the enterprise to compliance fines and costly breaches (average breach cost ~$4.35M).

Meet IDX, a next-generation workforce contractor identity solution based on the Accountable Digital Identity Association (ADIA) specification. IDX is purpose-built to close the contractor identity gap by delivering seamless integration, privacy-first biometric authentication, and AI-powered automation. The result: contractors get unique, verified identities that plug into your existing IAM ecosystem with little to no development effort, while your organization eliminates shared credentials, reduces risk, ensures compliance, and slashes IT overhead.

SEAMLESS INTEROPERABILITY WITH EXISTING IAM SYSTEMS

“No Rip-and-Replace” Integration: IDX was designed to work alongside your current IAM infrastructure, not replace it. Built on ADIA’s interoperability principles, it easily connects with identity providers like Microsoft Entra ID (Azure AD), Okta, ForgeRock, and Ping via standard protocols (SAML/OIDC) via SCIM. ADIA’s specification explicitly emphasizes interoperability so companies can adopt new reusable identity solutions without disrupting existing identity systems.

“Plug-and-Play" Deployment: Whether your enterprise uses cloud IdPs or on-prem directories, IDX natively synchronizes with them. It can connect to LDAP/Active Directory or HR systems to pull contractor rosters, then automatically provision and update identities in your IAM. The result is seamless adoption with minimal retraining or process change for IT teams and systems.

PRIVACY-PRESERVING BIOMETRIC AUTHENTICATION (NO DATA STORED)

Biometrics Without Compromise

IDX introduces strong biometric verification for contractors to ensure the person logging in is the one vetted, but it does so with a privacy-preserving approach. With authID's PrivacyKey™, biometric data is never stored in any cloud or IDX system. Instead, biometrics are replaced by a Private and Public key-pair, meaning no biometric data is retained. This architecture mitigates privacy concerns and eliminates the honeypot of centralized biometric databases. Even IDX itself cannot reconstruct or misuse a user's biometric info.

Zero PII Retention by IDX Interchange

All personally identifiable information (PII) collected during identity proofing (such as government ID scans used for verification) remains under the enterprise's control. IDX never stores PII in its cloud – sensitive data stays behind your firewall or is held only transiently for verification. This aligns with ADIA's privacy-by-design framework, where identity directories do not store any personal information about users. Once a contractor's identity is verified and linked to their digital identity, IDX discards any raw PII, keeping only a minimal digital identifier (e.g. a non-identifying digital address or DID). This approach helps enterprises to comply with GDPR, CCPA, BIPA since personal data isn't proliferated or retained unnecessarily.

Secure & User-Friendly Authentication

With IDX, your workforce authenticates with a combination of FIDO Keys on device and via a quick selfie matched to their verified identity using PrivacyKey – a process that is both highly secure and frictionless. Because no passwords are shared or reused and no username is issued, the risk of credential compromise is eliminated. Biometric login is tied to liveness and anti-spoofing checks, preventing imposters or sophisticated bad actors leveraging AI for Presentation Attacks or Deep Fake Attacks. Yet from the user's perspective, the authentication process remains easy, frictionless and respects their privacy. IDX effectively provides passwordless, phishing-resistant authentication, bolstering security without burdening the contractors or exposing your company to privacy liabilities.

AI-POWERED, ZERO-DEVELOPMENT ONBOARDING AUTOMATION

Automatic Contractor Enrollment

Say goodbye to slow, manual account setup for each contractor. IDX uses AI-driven identity proofing and workflow automation to handle contractor onboarding with little to no development effort. As soon as a new contractor is added to your directory or vendor management system, IDX AI Agent detects the entry and automatically creates a corresponding digital identity for that person in your IAM – no IT ticket or coding required. The platform's AI intelligently maps contractor attributes (name, role, department, etc.) from your source systems to the appropriate identity profile and access groups. This ensures policies (least privilege, RBAC rules, etc.) are consistently applied without IT having to intervene for each new hire.

Self-Service Identity Claim via Document Verification (Proof™) and HR Record Check

Once IDX generates a digital identity [DID], credentials are not activated until the contractor claims and verifies it. The contractor receives a secure invitation to initiate the process via a mobile app or web portal. Leveraging AI-powered document verification (Proof™), IDX prompts the user to scan a government-issued ID and complete a live biometric selfie. IDX not only validates the authenticity of the ID and matches the selfie to the ID photo but also extracts identity attributes and crossmatches them against the originating HR or directory record. This ensures that the individual claiming the DID is not only a real person, but the right person, the one who was hired. The entire process is automated: ID collection and authentication, liveness detection, biometric comparison, and HR record correlation are all handled without developer involvement or manual review. Once verified, the contractor's identity is cryptographically bound, and their access is activated in your IAM. If any verification step fails or flags a discrepancy, your security team is alerted. This end-to-end flow enables secure, policy-driven onboarding in minutes, with minimal operational overhead.

KEY BENEFITS FOR ENTERPRISES

IDX delivers tangible security and operational benefits that resonate with CISOs and IT leaders:

Eliminate Shared Credentials & Ghost Accounts

IDX replaces the outdated and risky practice of shared logins and generic accounts with unique, verifiable identities for every user, contractor, vendor, or employee. This ensures that every access attempt is tied to a real, verified individual, restoring accountability across the organization. When access needs to be revoked, deactivation is instant, precise, and secure, eliminating the risk of lingering accounts long after contracts have ended.

Reduce Security Risk & Prevent Credential-Based Breaches

With FIDO2 and biometric-bound authentication, IDX removes one of the most common entry points for attackers; compromised third-party credentials. Every login is strongly bound to a human, not just a username. This biometric link ensures that only the authorized individual can access systems, eliminating the probability of credential stuffing, phishing, and impersonation attacks. By closing this common security blind spot, IDX directly reduces the risk of catastrophic breaches, many of which originate through third-party access.

Ensure Compliance with Data Privacy and Access Standards

IDX is designed with regulatory alignment at its core. It supports compliance with standards like PCI DSS8, HIPAA, GDPR, and CCPA by enforcing unique identities, auditable access trails, and zero retention of personally identifiable information (PII). Its privacy-first design ensures biometric and identity data is processed securely and discarded after verification, never stored or exposed, helping enterprises adhere to data minimization principles and avoid hefty non-compliance fines.

Lower IT Overhead & Streamline Operations

IDX automates the entire identity lifecycle, from onboarding to deactivation, without manual IT intervention. Contractors and external users self-enroll through guided, AI-powered workflows, including document and biometric verification, reducing the burden on IT helpdesks and access management teams. This not only accelerates time-to-productivity for new users but also eliminates password reset tickets and orphan account audits. IT can shift focus from account hygiene to strategic initiatives.

Protect Corporate Data & IP

With fine-grained identities and access policies for contractors, you dramatically reduce the risk of data leakage or unauthorized access to sensitive systems. IDX ensures contractors only access what they're permitted and only for the duration needed – preventing the common issue of over-privileged third parties. This helps avoid incidents that could lead to IP theft or customer data exposure, safeguarding your business's critical assets

Accelerate Onboarding and Business Agility

In traditional environments, onboarding contractors can take days or weeks due to background checks, manual provisioning, and paperwork. With IDX, this process is reduced to minutes. The platform automatically provisions digital identities when new users are added to a directory and activates access only after identity proofing is complete. This agility is critical for dynamic workforces, seasonal staff, or urgent project-based hiring.

Improve Identity Hygiene Across the Organization

IDX ensures that every identity in your ecosystem, internal or external, is verified, current, and deactivated when no longer needed. This improves your overall identity hygiene and reduces the prevalence of shadow IT, orphaned accounts, and unmanaged identities. IAM leaders gain unified visibility across all users, enabling better governance and risk posture.

Build Trust with Contractors and Ecosystem Partners

By offering secure, user-controlled credentials, IDX positions your organization as a privacy-forward, security-conscious partner. Contractors and vendors receive credentials that are portable, professional, and interoperable, enabling a smoother onboarding experience and reinforcing trust in your processes. This improves partner satisfaction and cooperation, especially in compliance-driven sectors like finance, healthcare, and government.

Future-Proof Your Identity Strategy

IDX is built on the ADIA specification, designed to support decentralized, verifiable identity models that align with where the industry is heading. This means your identity infrastructure becomes extensible, ready to support future use cases like verifiable credentials for training, certifications, or cross-organization collaboration. It also ensures that your IAM strategy remains aligned with emerging privacy and identity standards globally.

Each of these benefits contributes to a stronger security posture and more efficient operations. For a CISO, that means fewer sleepless nights worrying about the unknowns of third-party access, and for IT, it means a cleaner, more manageable identity environment.

COMPETITIVE DIFFERENTIATION: IDX VS. TRADITIONAL IAM & SCIM

Beyond Employee-Centric IAM

Conventional IAM solutions (Entra, Okta, Ping, ForegeRock etc.) do a decent job at managing full-time employees whose data lives in HR systems, but they struggle with non-employee populations. Contractors often end up shoehorned via clumsy approaches – e.g. local accounts, ad-hoc SSO setups, or treated like full employees, each of which has downsides. IDX is purpose-built for this gap, delivering a solution that treats contractors as first-class identities without burdening HR or IT. Unlike traditional IAM, IDX doesn't assume a static HR feed or a pre-issued credential – it actively establishes trust in the identity through verification and then federates it into your IAM. This closes the identity proof loop that typical IAM/SSO leaves open for contractors.

Augmenting (Not Replacing) Your IdP

It's important to note that IDX is not an IdP suite replacement, but an overlay service specialized for contractor identity challenges. Many organizations attempt to use SCIM-based provisioning from an HR or vendor system to create contractor accounts. However, SCIM alone has limitations for this use case – it was designed for straightforward data sync, not for identity vetting or complex invite or onboarding workflows. For instance, SCIM assumes a user is created instantly when provisioned, whereas contractors often need an invite and acceptance step; this mismatch require clunky workarounds. IDX improves this by seamlessly handling invite/claim flows – a contractor identity in IDX isn't active until verified, and yet this process is invisible to your IdP until completion, so your directories stay clean and accurate. Furthermore, SCIM provisioning generally won't validate that "Jane Doe the contractor" is who she claims – it just creates an account. IDX adds an identity assurance layer on top of provisioning, using document and biometric checks to ensure each account corresponds to a real, authorized individual. In essence, IDX + your existing IAM gives you the benefits of a decentralized, verified identity framework (as envisioned by ADIA) using the systems you already have.

Differentiators at a Glance

- **Integrated Identity Proofing:** Unlike standard IAM or MDM solutions, IDX bakes in identity verification (ID + biometric). This drastically reduces impersonation and fraud risk (a contractor can't share their login or pretend to be someone else).
- **Privacy & Decentralization:** Traditional IAM might require copying personal data into various systems or the cloud. IDX, built on ADIA principles, keeps PII local and identities user-controlled, which is a unique value prop in an era of rising privacy mandates.

- **AI Automation:** Competing approaches often involve custom scripts or manual onboarding for contractors. IDX's AI-powered workflows mean it's largely hands-off for IT – a capability legacy IAM tools don't provide out of the box.
- **Rapid Deployment:** Thanks to its open-standard ADIA foundation, IDX can be deployed quickly with minimal configuration. For example, the ADIA reference implementation demonstrated integration with just a few simple API calls. Compared to lengthy IAM migrations or custom development for provisioning, IDX delivers value in days, not months.

By improving on these fronts, IDX represents a leap forward in managing external identities – it's like going from a patchwork of manual processes to a cohesive, intelligent system purpose-built for the modern extended workforce.

IMPLEMENTATION STRATEGY: QUICK ADOPTION WITH MINIMAL DISRUPTION

Adopting IDX is designed to be straightforward and low-risk for enterprises. A typical deployment strategy is:

1. **Pilot in Parallel:** Start with a pilot group of contractors or a particular vendor. IDX can be layered on in parallel with your current IAM – for example, for a subset of applications or a specific department's contractors. This allows you to validate integration and user experience without impacting all users at once. Because IDX uses standard SSO integration, contractors in the pilot will log in via your existing SSO portal (now backed by IDX for their identities) seamlessly.
2. **Simple Configuration, No Code Changes:** Your identity administrators configure IDX via a management console to connect to your directories (e.g. read-only service account for LDAP or an API token for Entra/Okta). Out-of-the-box connectors and templates make this step quick. No application code or custom plugins are required – existing SAML/OIDC federation is used for authentication, and SCIM/Graph API for provisioning if needed. As ADIA's modular design showed, integration can be achieved with minimal engineering effort, often just mapping attributes and defining workflows rather than coding.
3. **On-Premise or Cloud Flexibility:** For organizations with strict data policies, IDX components responsible for handling PII (like the document verification service) can be deployed on-premise or in a private cloud. Meanwhile, the orchestration and non-PII identity data can reside in the IDX cloud service. This hybrid deployment ensures no disruption to network policies – all sensitive operations happen behind your firewall, maintaining the same security perimeter as your current identity stores.

4. **Gradual Rollout and Integration:** Once the pilot is successful, broaden IDX to more contractor groups and integrate more applications. Thanks to its interoperability, IDX can gradually absorb the contractor identity management for various business units without a "big bang" cutover. You might phase it such that new contractors use IDX from a certain date forward, while legacy contractors are migrated during their re-validation or contract renewal. The phased approach ensures business continuity – there's always a fallback (existing access) until each user is verified in IDX.
5. **Training & Change Management:** From the contractor's perspective, using IDX is simple (click a link, verify identity once, then SSO as usual but with biometrics). Internal staff (like hiring managers or vendor managers) will need minimal training – mostly on how to trigger invites or check status in the IDX dashboard. Because IDX aligns with familiar SSO login flows and automates admin tasks, the change management is minimal. Enterprises often find that contractors appreciate the professionalism of being given their own credentials rather than shared ones, improving cooperation and security culture.

Minimal Disruption, Maximum Security

Throughout the implementation, your existing IAM remains the source of truth for access policies. IDX feeds into it, so there's no abrupt switch for access control. This means no downtime and minimal risk during deployment. Essentially, IDX slips into your IAM stack like a new layer of security and automation, quietly upgrading your contractor's identity process without disrupting ongoing operations. Enterprises can typically get IDX up and running in weeks, and because it's largely configuration-driven, adjustments post-deployment (e.g., tweaking workflows or adding new ID types) are quick and do not require major projects.

ROI AND SECURITY IMPACT METRICS FOR CISOS

Investing in IDX yields measurable returns in both risk reduction and cost savings. The key metrics to consider include the following points.

Reduction in Breach Likelihood

By closing a common attack vector (third-party credentials), IDX can significantly reduce your organization's breach likelihood. Considering that 62% of network intrusions stem from third-party access, even cutting this risk in half has a massive impact. A conservative estimate might be a double-digit percentage reduction in overall breach risk. If your company's average cost per breach is, say, $5M (industry average), preventing even one major incident through stronger contractor security yields immediate ROI that dwarfs the cost of IDX.

Eliminate Account Takeover/Fraud Incidents

Metrics around account takeover (ATO) or misuse of contractor accounts will improve. For example, if you previously had N number of security incidents or support investigations per year related to contractor accounts (shared password use, unauthorized access, etc.), expect that to go to zero. Each avoided incident not only saves incident response effort but also protects against potential losses.

Time-to-Onboard Improvement

From an operational efficiency standpoint, measure the time to onboard a contractor before and after IDX. If onboarding a contractor (from request to active access) took days or weeks due to paperwork and manual setup, with IDX that can drop to hours or minutes (since identity verification and provisioning are automated). Faster onboarding can be quantified in productivity gains for both the contractor (who becomes productive sooner) and the managers waiting for them to get access. This is crucial for contracting firms where delay equals lost productivity or revenue.

IT Man-Hours Saved

Calculate the reduction in IT helpdesk and administration hours. Each contractor typically required a certain amount of IT touch (account creation, password resets, access adjustments, deprovisioning audits). With IDX automating provisioning and offering self-service biometric login (no more password resets), these touches are minimized. Enterprises have found that automated provisioning can reduce IT workload for user management by 50% or more – freeing up IT staff for strategic projects. For instance, if your IAM team spends 100 hours/month on contractor account issues, IDX could cut that to a fraction (translating to tens of thousands of dollars saved annually in support costs).

Compliance and Audit Savings

With IDX's detailed logging of identity verification and usage, preparing for audits (internal or external) becomes easier. Metrics like "% of contractor accounts with verified identity proof" will be 100%, demonstrating strong controls. This can speed up compliance audits (reducing compliance staff time) and avoid costly findings. Furthermore, avoiding compliance penalties (which can reach millions in sectors like healthcare or finance) provides a significant risk-adjusted savings. For example, HIPAA violations for failing to properly secure access can incur fines – having IDX as a compensating control reduces the likelihood of such fines to near zero.

Lifecycle Management Efficiency

Track the improvement in deprovisioning speed. IDX's continuous sync ensures contractors are disabled as soon as their engagement ends (or even automatically expire on a set date). This eliminates lingering access. Metrics to watch: number of orphaned contractor accounts pre-IDX vs. post-IDX deployment. Reducing those to zero not only improves security but saves the effort of periodic account clean-ups and potential costs of excess license usage on SaaS apps.

In summary, the ROI of IDX is realized through risk reduction (preventing expensive breaches), IT cost savings (automation and efficiency), and improved business agility. An investment in IDX can often pay for itself within the first year when you consider the cumulative savings: fewer incidents, lower labor costs, and avoidance of even one security catastrophe or regulatory fine. For the CISO, these metrics translate into a strong business case – stronger security and lower operational costs is a win-win that is hard to achieve with most security investments. IDX manages to do both by fundamentally improving how you handle identities that were previously a weak link.

CONCLUSION: STRENGTHENING TRUST IN THE EXTENDED WORKFORCE

In today's threat landscape, identity is the new perimeter – every person with access to your network must be accounted for and secured. IDX, guided by the ADIA specification's emphasis on accountability, privacy, and interoperability, allows you to extend a "Zero Trust" identity model to your contractors, customers and partners with ease. It integrates effortlessly with your existing IAM, respects user privacy by design, and leverages AI to eliminate tedious workflows. The result is a more secure enterprise where only the right people – and actual verified people – have the right access at the right time, no matter if they're full-time employees or third-party contractors.

For CISOs, IDX offers a compelling proposition: a solution that plugs a known security gap, aligns with modern privacy standards, and delivers immediate operational value. By adopting IDX, you're not just buying a product, you're embracing a new paradigm of digital identity – one that can evolve with your organization's needs and the changing regulatory environment (thanks to the vendor-neutral ADIA framework behind it). It's a strategic investment in fortifying your defenses and future-proofing your identity infrastructure.

IDX turns contractor identity management from a liability into an asset. We empower your security team with visibility and control, your IT team with automation, and your contractors with a seamless yet secure experience. The business can confidently leverage third-party talent and services without introducing unacceptable risk. In an era where trust and accountability are paramount, IDX ensures that every identity accessing your enterprise is one you can trust – and verify. It's time to close the contractor identity gap and strengthen your enterprise's security posture with IDX.

ABOUT AUTHID

authID (Nasdaq: AUID) helps enterprises “Know Who’s Behind the Device™” with a patented biometric identity platform that delivers lightning-fast identity proofing, authentication, and account recovery. Powered by PrivacyKey with no biometric data stored, authID blocks deepfakes, prevents account takeover, and eliminates password risk, enabling the most secure and seamless user experience in the digital ecosystem.