



indicio

An Introduction to Decentralized Identity in 2026

It's **the** year for portable, privacy-preserving, and seamless digital trust — here's what you need to know.

By Trevor Butterworth & Helen Garneau

The world is pivoting to decentralized identity

In 2025, identity fraud evolved much faster than the technology to combat it. Legacy authentication systems were assaulted by continuous, adaptive AI-powered fraud that deployed fake documents and deepfake biometrics.

Not only is this new tech able to defeat many KYC (Know-Your-Customer) processes, it is able to learn from its failures. A Gartner survey [found](#) that 62 percent of organizations had experienced a deepfake attack in the past year.

The global cost of digital fraud in 2025 was estimated by Infosecurity Magazine at **\$534 billion dollars**, a cost that will likely increase, if we continue to stick with the same-old same-old identity authentication processes even as we add millions, potentially billions, of device, robot, and AI agent identities.

There is no magic amount of multiple factors to protect against the built-in vulnerabilities of systems that rely on centralized data, logins, and passwords.

This is why, in 2025, the world started to take decentralized identity seriously by implementing it for travel, KYC, and account access.

Tldr: it removes the vulnerabilities that sustain digital fraud just as removing pools of standing water gets rid of mosquitoes.

It would be an amazing technology if it only did just that, but decentralized identity is more than identity authentication, more than a preventative solution.

What makes it so powerful is that **it radically simplifies how we share and act on data**, infrastructurally, operationally, and in terms of user control and experience. It's a way to automate and facilitate trust — and that delivers business and organizations benefits in addition to security.

This paper will take you through the tech, what it means, how it is being used — and most importantly, how you can use it to prevent your 2026 bottom line from becoming next year's data point in the digital fraud statistics.





Part 1: What is decentralized identity?

What is Decentralized Identity?

Instead of verifying someone's personal data — their login, their password — by checking it against the same login and password stored in a central location, the person holds their data and is in full control of it. When they consent to share it for verification, it can be independently verified using cryptography.

There's no need for cross-checking with a database, a third-party identity provider, or "phoning home" to the original source of the data to ask if it's authentic. The data presented by a person can be independently authenticated.

The key to this is a verifiable digital credential, a collection of data that's digitally signed in a digital container that's digitally signed.

Any document or record can be turned into a Verifiable Credential: a passport, citizen identity document, driver's license or membership card.

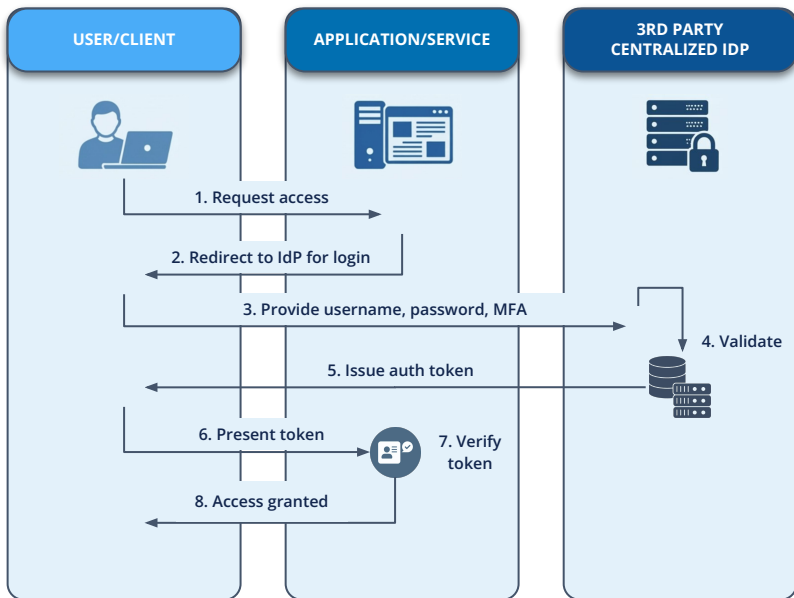
There are some limitations on the size of a credential: Medical images such as a CT-Scan or MRI are too big to put in a credential but not biometric templates or photographs of documents.



Decentralized means giving people organizations or even devices control over their own data. This means data that's fully portable and that requires the person's consent to it being shared.



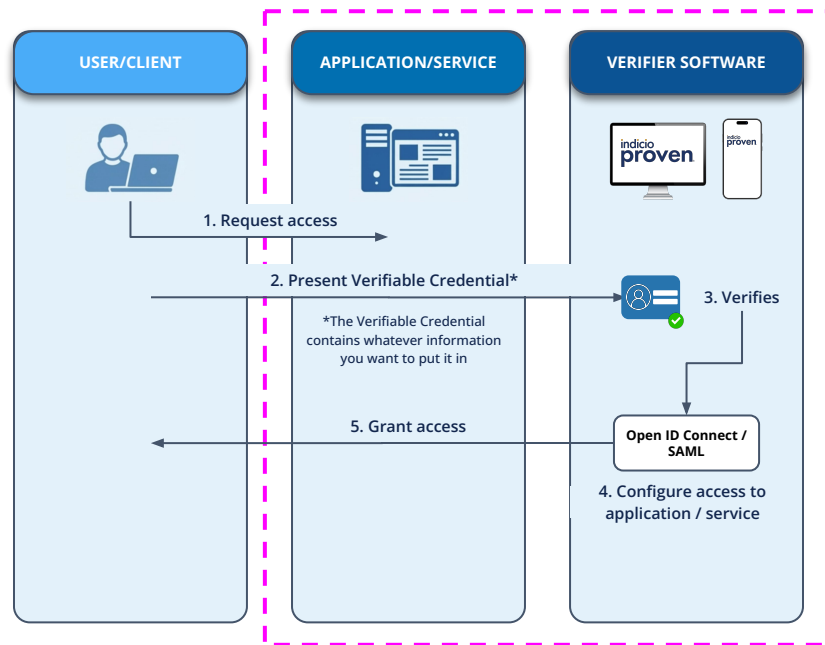
Centralized identity



Decentralized identity turns this ^

vs

Decentralized identity



...into this ^

Which means no need for usernames, passwords, MFA, an IDP provider or database of personal data to validate credentials.

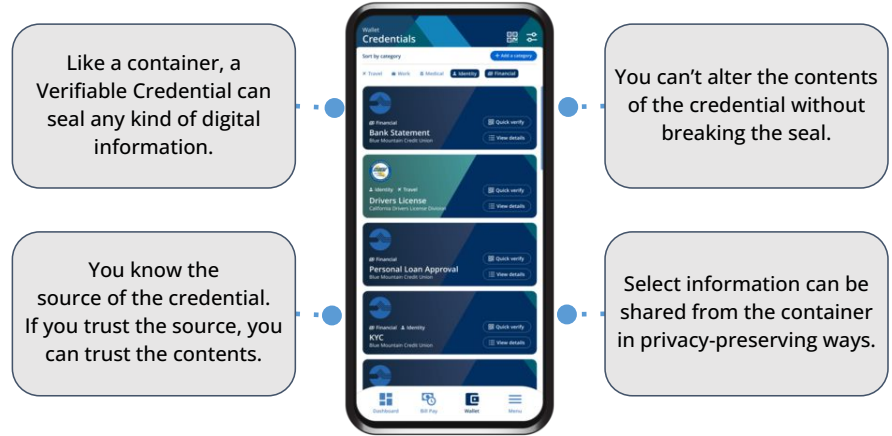
What makes a credential a *Verifiable* Credential?

We capitalize “**Verifiable Credential**” for a reason. There are lots of digital credentials in the marketplace, and many of them are described as “verifiable;” but this doesn’t mean that they’re technically Verifiable Credentials.

Verifiable Credentials are fully decentralized. This means the data they contain is independently verifiable. There’s no need to phone home (to the original issuer) or cross check against the same data stored by a third-party to see if its correct.

Verifiable Credentials are held in digital wallets on mobile devices and not in a centralized database by a third party. This removes the risk of honeypots of personal data being stolen in a data breach, and it also means that data must be shared by the consent of the data holder — a transformation in data privacy.

The information in the credential is digitally signed. This means you can cryptographically prove who signed it and that the information hasn’t been altered.

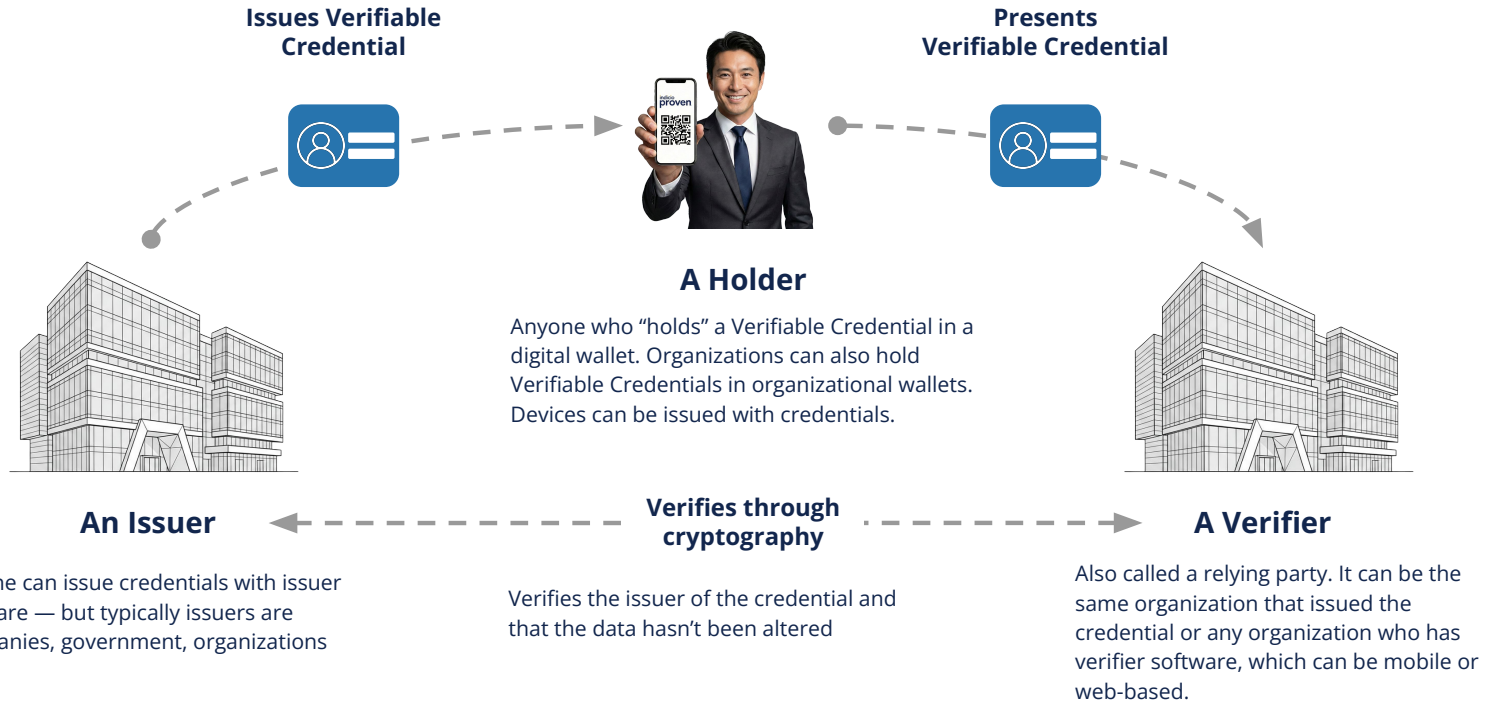


A Verifiable Credential is like a digital container.

Similar to the way standardized shipping containers transformed trade, VCs are a **highly efficient** way to share data **from anywhere to everywhere**, reducing the uncertainty as to the data’s origin and integrity and thereby allowing the data to be immediately used.



Issue, hold, present, verify



No need for usernames, passwords, or MFA

Decentralized identity radically simplifies authentication. There is no longer any need to store vast amounts of personal data to authenticate someone's identity — and if personal data doesn't need to be stored it can't be stolen.

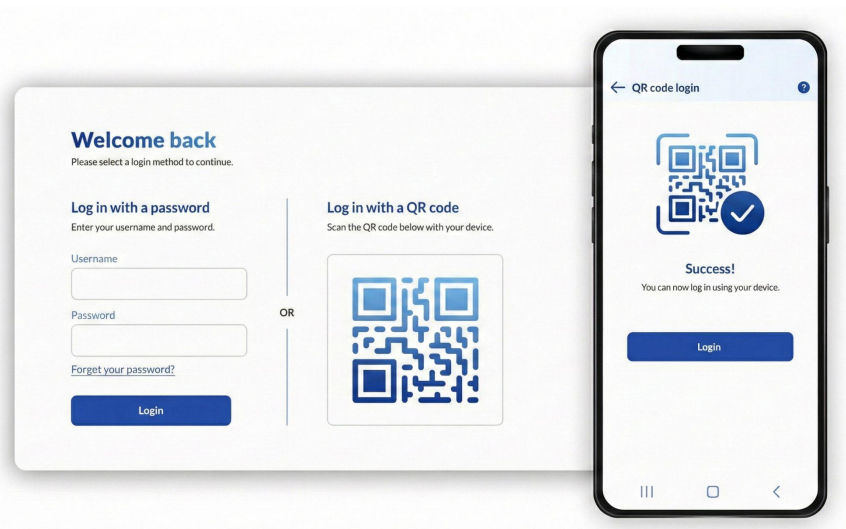
There is no longer any need for logins and passwords, which means they can't be faked or guessed or stolen. Sometimes the best way to tackle a vulnerability is to completely remove it.

Issuing, presenting and verifying credentials and their data is initiated by issuing or scanning a QR code or link.

Mutual authentication

Verifiable Credentials come in different formats. Those that use decentralized identifiers (DIDs) have a special and powerful communications feature. It's instant, but it's easier to understand it as a two-step process.

Step one: when you scan a QR code to receive a credential or present a verifier with a QR code for them to scan, you set up a secure communications channel directly with the other party.



When this happens, you and they cryptographically prove that each of you is in control of the end of their channel.

This means each party can be absolutely certain that the messages in this channel are coming from each end of the virtual line. This represents a massive security upgrade to digital interaction.



A massive security upgrade

In many cases, such as customer-business interactions, this step may be sufficient. The business identifies itself with a public DID and that is a sufficient proof of its identity: no other business will have the same public identifier, and governance tells your software that this business is trusted (we're simplifying this for the sake of brevity).

But there are many instances where being able to prove control of an identifier is not the same thing as proof of identity.

This takes us to **step two**, where we determine “who” we are interacting with through a Verifiable Credential. Now we go from knowing that someone controls the other end of the virtual line to *knowing exactly who that someone is* (because we have verified the source of their credential). Combined, these steps function like a force field against being phished or bot impersonations.

Importantly, none of these communication channels can be correlated. Say, you use one credential to prove your identity to access forty different e-commerce sites. Each individual interaction is going to have a uniquely encrypted communications channel for you to conduct business. This means you can't be tracked across platforms.

Different communications protocols offer different features. The most advanced — **DIDComm** — provides a powerful way to personalize interaction, because it's capable of rich communication.

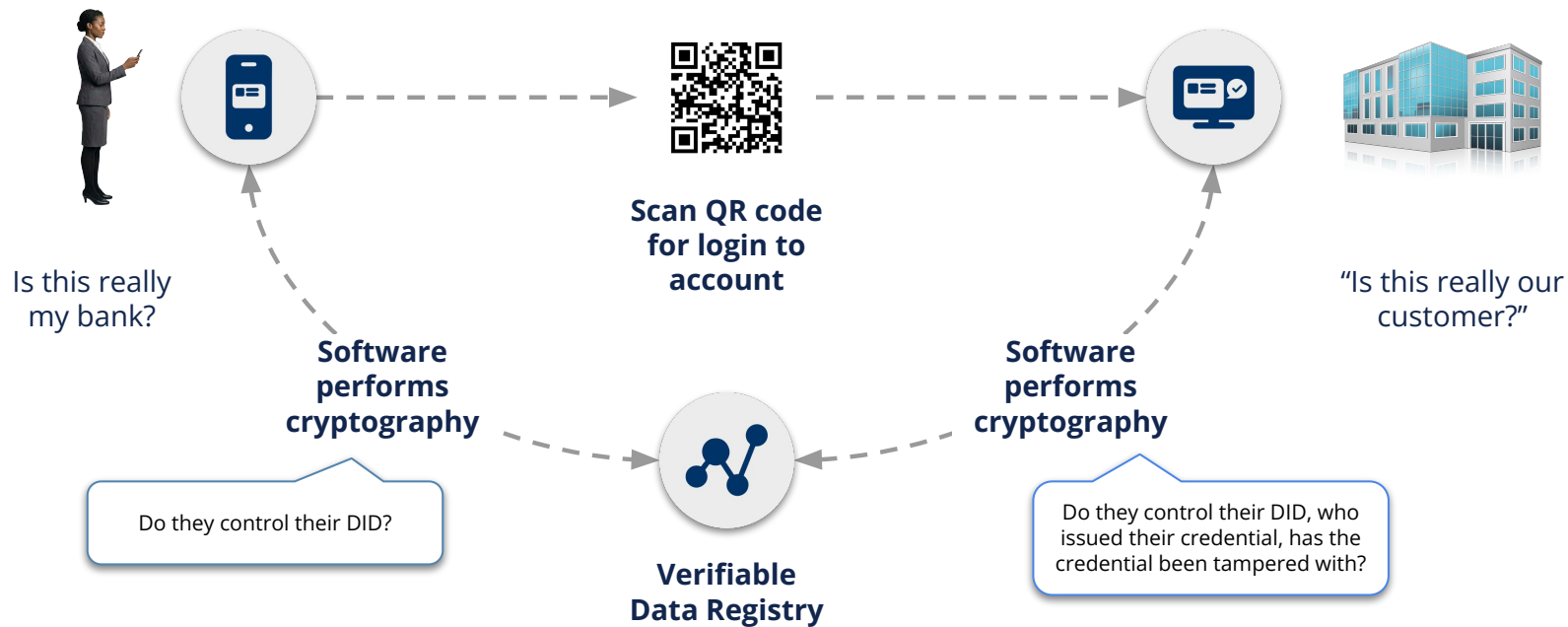
The net result is that when you combine secure authentication with secure, peer-to-peer communication, you are able create the virtual ground for digital relationships.

This has immediate relevance for things like managing loyalty programs; but it's a capacity with transformative potential as people explore decentralized identity beyond secure authentication.

The combination of a secure communications protocol and verifiable identity is a way to create trust between parties who otherwise have limited or no connection to each other — and this is a powerful way to generate markets.



Example: Logging into a bank account



This contains only the information needed to perform the cryptography (and also to check whether the credential has been revoked).
Can be ledger-based or ledgerless

How do we know which Verifiable Credentials to trust?

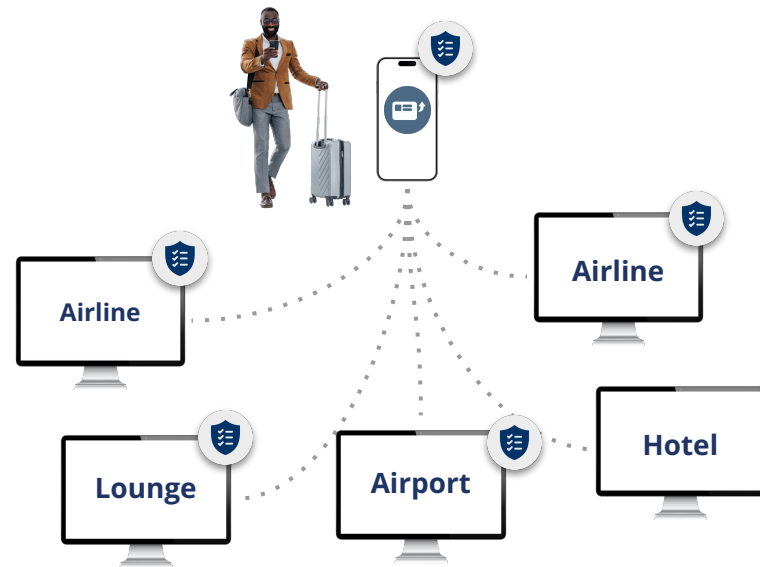
Decentralized identity allows us to easily make decisions about who and what to trust and automate these decisions for instant authentication and seamless processes.

If you can instantly know the source of a credential and you trust that source — for example, an airline, a bank, a school, a government — you can trust the information inside the credential because you can also prove it hasn't been altered since it was issued.

But how do you scale this trust when there are many credential issuers and many more verifiers? The answer is governance.

Decentralized governance provides machine-readable lists of trusted credential issuers to every credential holder, so they are able to know who's in the trust network and who isn't. Similar lists can be published for verifiers, so a holder can know, for example, that a tour guide or service has been approved within a tourist app.

These governance files are decentralized because they are downloaded by everyone in the credential ecosystem. They tell people's software which credentials are trustworthy because the issuer has been vetted by the authority who created the credential ecosystem.



An example of a decentralized governance file coordinating credential verification in a travel ecosystem

Indicio's governance solution is based on the global [Credential Trust Establishment](#) specification by the Decentralized Identity Foundation.



What happens if I lose my phone?

First, a person can't share or loan credentials that have been issued to them with others to use. It is also possible to bind credentials to the person that they were issued to in the AnonCreds credential format.

They're accessed through a phone's biometric or code with a second line of biometric or code access to a digital wallet. This combination is highly efficient defense against hacking or phishing.

A credential can't be stolen from a person's digital wallet as each credential is bound, cryptographically, to the wallet it was issued to. Even if a thief could steal a credential they couldn't present the data from it and have that data verified.

AI can't fake a credential by re-engineering the digital signatures that bind the credential to its issuer and "seal" the data inside."

If a credential holder loses their phone, the credential is gone. It should be formally revoked, and it has to be reissued (by meeting the identity assurance requirements that allowed it to be issued in the first place).



AI can't fake a credential by re-engineering the digital signatures that bind the credential to its issuer and "seal" the data inside."

Taking Verifiable Credentials to the next level: Adding biometrics

A few years ago, biometrics became “the solution” to the problem of authentication. Your face can be your password. Yay.

The world invested billions of dollars in biometric systems, and then AI arrived and rapidly made it easy and then routine to fake biometrics.

You could reset a password; but how do you reset your face? Deepfakes are widely seen as an existential threat to business.

The solution? Put your face or fingerprint or voice in a Verifiable Credential. Either capture a biometric during identity assurance or derive one from a known, authenticated biometric, such as the image in a passport chip.

Now, any liveness check can be cross-checked against the supposedly “live” person by asking them to present a Verifiable Credential. If their liveness check matches the authenticated biometric in their credential, they are not a deepfake.

Simple, fast, cost effective, tamper-proof — and the highest level of digital identity assurance.

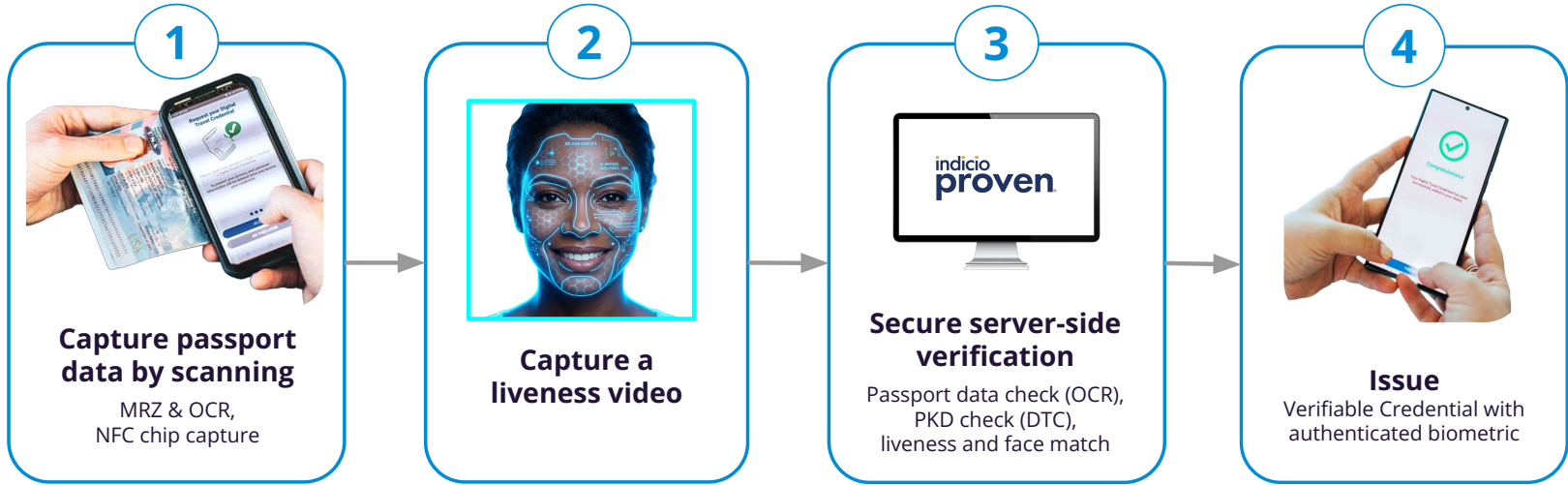
But Verifiable Credentials do more than save biometric infrastructure, they make biometric authentication simple, privacy-preserving, and portable.

You no longer need to store biometric data (and deal with the integration, compliance, and security challenges and costs) to verify it — a major breakthrough.

This means that Verifiable Credentials allow biometric authentication to become a new, global standard for routine identity authentication, better than before, stronger, faster — the world’s strongest digital identity.



How to create world's most powerful digital identity in minutes (with Indicio Proven®)



Indicio software scans and ingests the data embedded in the passport chip, and optically reads the printed data in the passport.

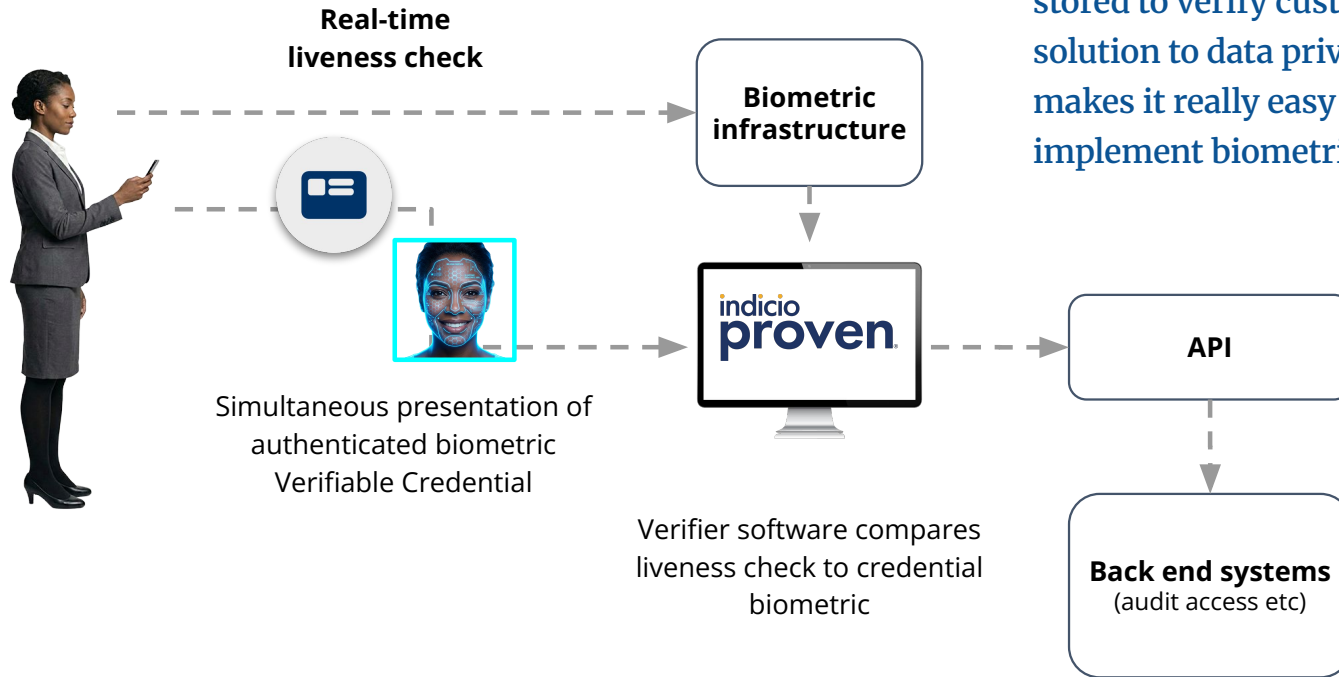
The person takes a liveness video of themselves. State-of-the-art face-mapping software from Regula will compare this image with the embedded image from the passport chip to ensure they represent the same person.

Regula validates the identity document is authentic.

The issued credential cannot be shared or stolen or faked. When they present the credential, simple verifier software can cryptographically prove who issued it and that the data hasn't been altered.



Authenticated biometrics in VCs bypass deepfake threat



No biometric data needs to be centrally stored to verify customer biometrics — a solution to data privacy regulation that makes it really easy for anyone to implement biometric authentication.

What decentralized identity means for privacy

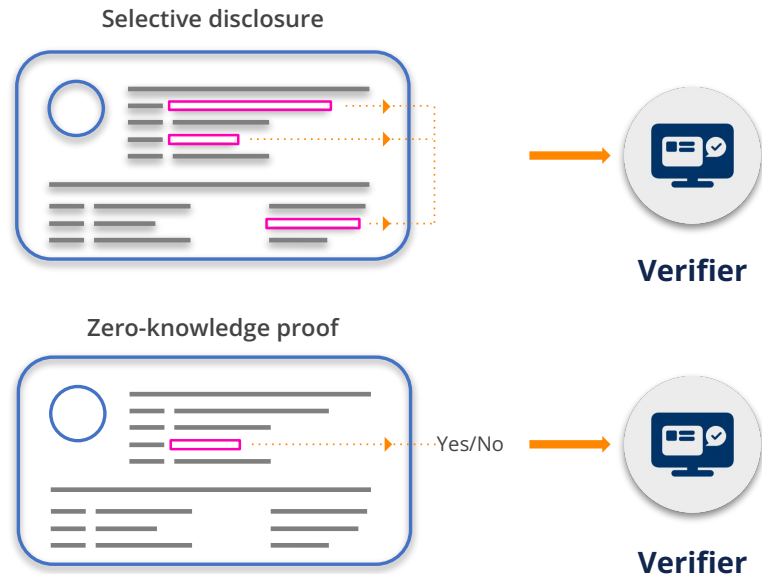
Decentralized identity and Verifiable Credentials are built on **privacy-by-design** principles. Because a person — a data subject — holds their personal data and biometrics, they control who they share it with. Consent is built into interaction.

Relying parties don't need to hold this data in storage to establish its validity (i.e., where the information came from and whether it has been altered post issuance to a credential).

This maximally achieves the principles articulated in Article 5 of GDPR: No personal data needs to be stored outside of specific legal requirements in order for it to be verified (data minimization); data can be shared selectively and in privacy-preserving ways (data minimization); the data is required for a specific purpose only (purpose limitation).

At every step in data processing, clear, informed consent is required from the data subject to accept a credential and to present information to a relying party from a credential.

This consent can be recorded for audit, making the compliance auditing requirements of GDPR easy to meet.





Part 2:
**What do Verifiable Credentials mean
for business?**

Digital transformation without rip and replace

Decentralized identity can be thought of as **a technology layer** that you **add to systems** rather than a solution that replaces systems. This is critical from a cost and logistical perspective. You can decentralize what you have at a pace that's manageable, rather than commit to the terrifying prospect of a massive IT replacement project.

A simple implementation can take days (such as converting Auth access to a Verifiable Credential). A more complex implementation, such as a national border can take a few months.

What this means, practically, is that an organization can **start small**, learn how the tech works, see value rapidly, and **scale at their own pace**. This is how Indicio's customers have all succeeded in deploying Verifiable Credentials.

As decentralized identity technology is built on **open standards** and follows **global specifications**, it's able to work across industries, devices, and borders, while evolving to incorporate new features, and facilitate new requirements and regulations. This makes it sustainable and future-proof. Organizations grow as the tech evolves instead of sinking money in systems doomed to obsolescence.



Create seamless operations, experiences

Verifiable trust creates customer data that can be instantly acted on — coupled with the permission needed for those actions to be compliant with regulations like GDPR. This makes Verifiable Credentials **catalysts for seamless interaction**.

For customers, digital interaction is effortless, a single, continuous journey and not a series of handoffs or roadblocks between different channels, departments, or organizations, each requiring re-authentication and repeated information.

For organizations, the ability to **unify customer data** across this journey and in real-time creates opportunities for a new level of personalization, relevancy, customer insight, and the opportunity to deliver new tailored products and services.

From an operations perspective, Verifiable Credentials provide a fast, secure, and cost-effective way to integrate customer data, departments, resources, and systems — and to apply consistent branding and experience across every interaction.



A credential ecosystem is a market for trusted data

Data that can be instantly acted on because it can be instantly trusted is a catalyst for digital markets, reducing risks and transaction costs.

Know-Your-Customer (KYC) processes are executed using biometric and document validation technology instead of photocopies and paper documentation that are highly vulnerable to fraud.

Global standards and interoperable specifications enable verifiable identities and data to be instantly consumed across sectors and borders simplifying interaction while also meeting AML/KYC and other regulatory requirements.

Low-trust business environments can be injected with high-trust data, facilitating collaboration between companies, access to financial services, and increased economic activity.

Payments and billing can be secured against identity theft and credit card fraud.

Remote areas can be connected in secure ways without the need for expensive centralized infrastructure.

A trust network for business and financial services can be run through mobile phones.



Identity authentication for AI and autonomous systems

Verifiable Credentials provide a way to authenticate the “identities” of connected devices, objects that have been made digital through multiple sensors, digital twins and their components, and most important of all, **AI agents**. Just like people, all these digital entities can be faked.

Verifiable Credentials authenticate AI agents as they do people. A customer can prove that an AI agent was issued with an identity by the organization it purports to represent.

An AI agent can prove that the customer is, in fact, a legitimate customer. They mutually authenticate each other before the customer consents to share their data, a critical step to ensuring these systems comply with data protection law.

The customer can also **delegate authority to an AI agent** to use their data across systems, sharing it with other AI agents (that the AI agent is able to authenticate as valid agents because they too have Verifiable Credentials).

By solving the authentication problem, and providing a way to meet data protection requirements, **Verifiable Credentials make AI systems practical, implementable, and interoperable.**





Part 3:
**The business sectors leading
decentralized identity adoption**

The business sectors leading the global adoption of decentralized identity

Banking and financial services

KYC (Know Your Customer)
AML (Anti Money Laundering)
DeFi (Decentralized Finance)
Payments.
Account access.

Verifiable Credential with authenticated biometrics dramatically improve KYC in terms of the quality of identity assurance and the speed of KYC processes.

Instead of taking days and relying on paper documents increasingly at risk of being faked with AI, identity can be quickly derived from government-issued identity documents by validating those documents and validating the person's biometrics (liveness check and face mapping) in minutes.

And by enabling digital identity assurance without the need to store personal data, it delivers on privacy, simplifies compliance, and removes a key security vulnerability.

Real-world example: Indicio customer onboarding in fintech

A global fintech company that relied on manual KYC checks—scanning IDs, uploading documents, live webcam sessions—faced high costs and high abandonment rates. With Indicio Verifiable Credentials, onboarding went from days to minutes. Compliance costs fell as repetitive checks were eliminated, manual reviewers were freed up for higher-value work, and customers enjoyed a seamless experience. Conversion rates jumped, repeat usage increased.



The business sectors leading the global adoption of decentralized identity

Travel, tourism, hospitality

Digital Travel Credentials
ETA, eVisa, and pre authorized travel
Loyalty program management
Check-in, baggage management, lounge access.
Duty-Free management
Border control
Car rental, hotel check-in.
Tourist apps and services

The International Civil Aviation Organization (ICAO), the global organization responsible for passport standards, published a set of specifications for Digital Travel Credentials — in essence, digital passports. The most developed specification is the DTC-1, which covers how to derive a Digital Travel Credential from a valid passport. This has become the de-facto standard for the application of decentralized identity to travel and tourism.

The driver is the projected increase in annual air passenger volume by 2040. people. It's expected to double to eight billion people — and Digital Travel Credentials are absolutely critical to managing increased capacity (in addition to all the security benefits).

By removing manual authentication touch points and enabling more of the approval and authentication process to happen before the traveler reaches the airport, Verifiable Credentials are able to speed up lines, reduce check-in space, and speed up border crossing.

Real-world example: Aruba

In deployment in Aruba, Digital Travel Credentials developed by Indicio for SITA, enabled travelers to cross the border in seconds — up to four times faster than alternative technologies.



The business sectors leading the global adoption of decentralized identity

Travel, tourism, hospitality II

Payments and fraud
Automation
Enhanced personalization
Real-time data access
AI agent authentication and permissioning

The global hotel and hospitality sector is expanding as people prefer to invest in experiences over things. At the same time, expanding tourist economies are hitting demographic challenges with worker shortages. Hotel check-in is a critical capacity blocker that can be automated with a verifiable digital identity combining a biometric. The automation simplifies operations and streamlines the guest's experience.

The same digital identity can be used to authorize hotel payments, thereby mitigating buyback fraud. It can be used to manage robot-guest interactions, and permissioned access to real-time wearable data for personalized services.

And if you can turn a hotel environment into a secure, streamlined privacy-compliant trust network where data can be instantly acted on without needing to be centrally stored, why not do the same for an entire tourist economy?

Now tourist authorities can use Digital Travel Credentials to integrate the entire tourist experience from pre-authorized travel to departure. Add licensed tourist services, in-app payments where there is a risk of using credit card payments.

Leverage permissioned data access for personalization.



Enterprise use cases

SSO

Simplify onboarding

Manage employee access

Simplify zero trust

Certification and licensing

Vendor identity

Verifiable billing and payments

Employees, contractors, and vendors can prove identity or authorization without relying on stored credentials that invite data breaches. This protects against phishing, fake invoices, and fraudulent vendors, while also making workforce onboarding faster. Because credentials integrate with identity systems like Keycloak, orchestration remains simple.

For single sign-on, Verifiable Credentials offer portability and flexibility that passkeys alone cannot provide, since they can be issued by the enterprise themselves and manage access at scale. A single Verifiable Credential can be used to orchestrate access to an entire suite of SaaS applications — and a company can configure access to trusted credentials that it did not issue.

Real-world example: Indicio customer and IAM

A large enterprise struggling with password resets, expensive IAM licensing, and weeks-long onboarding turned to Indicio. By shifting from usernames and passwords to portable credentials, IT support tickets plummeted, licensing costs dropped, and new hires were productive within days. Employees and contractors noticed the difference, reporting smoother, more secure access. What was once a cost and security drag became a competitive advantage.





Part 4:
Ready to start?
Here's what you need to know

Five reasons not to DIY

You could build your own from scratch — have your developer team learn the codebases and standards, develop all the elements needed for interoperability and functionality at country level scale, or you could implement and be up and running in days with **Indicio Proven®**.

Obviously, we think you should choose the latter option! But here are five reasons not to go it alone at this point in the market.

1. It's going to take time to **master all the codebases**. We have five years+ on your team — and many of our engineers contributed to the codebases.

2. You don't have years to figure this out. By the end of 2026, the EU has mandated that every one of its citizens, residents, and businesses have access to a digital wallet for using Verifiable Credentials — and this is to say nothing of global adoption. Recent reports from **Gartner** and **Jupiter Research** both note the scale of benefits provided by the technology and the **rapid pace of adoption**.

3. We know your engineering team is good. But there are two technical areas that **we have repeatedly seen teams derail on: interoperability and scale**. We've talked about the importance of interoperability, but scale — the ability to manage tens of thousands of credential issuances and verifications simultaneously — is equally important. The stumbling block is that mobile devices don't have fixed IP addresses — so how do you manage communication? Both are critical market advantages

4. The market is... now. And **you can be in it in a matter of weeks**. Why start on building the basics when you can also have the advanced features — interoperability and scale — and crucial partner integrations like document validation in weeks? Focus on building the business use case, not rebuilding the tech from scratch.

5. Building from scratch will cost you far more than buying off-the-shelf.



Indicio Proven® does everything you've read so far — and more

Indicio Proven is more than a platform: It is a **complete, interoperable, standards-based solution** for implementing decentralized identity with multiple credential types and protocols from mobile driver's licenses to Digital Travel Credentials.

It's **fully compatible** with the **European Union's** new digital identity specifications and digital wallet — and it enables EU-credential standards to work seamlessly with global credential standards for a true “from anywhere to everywhere” experience.

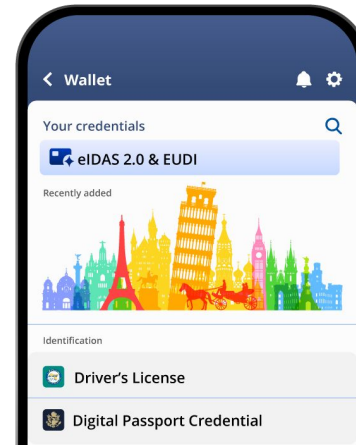
Proven is easy to use and **integrates seamlessly into existing workflows** and IAM systems, mobile applications, and cloud environments through a simple **API** and a **mobile SDK**.

Proven also delivers the broadest assurance capabilities through **our partnerships** with the world's leading document authentication, biometric services, and hardware providers.

Proven has **document authentication** built in so virtually any government-issued identity document worldwide can be authenticated and turned it into a secure, Verifiable Credential.

And it delivers the highest possible digital identity assurance by enabling **biometric authentication** and incorporation into Verifiable Credentials.

Together, these integrations give organizations confidence that their credentials are both genuine and bound to the right individual, closing off common attack vectors like deepfakes, synthetic IDs, and document forgery.

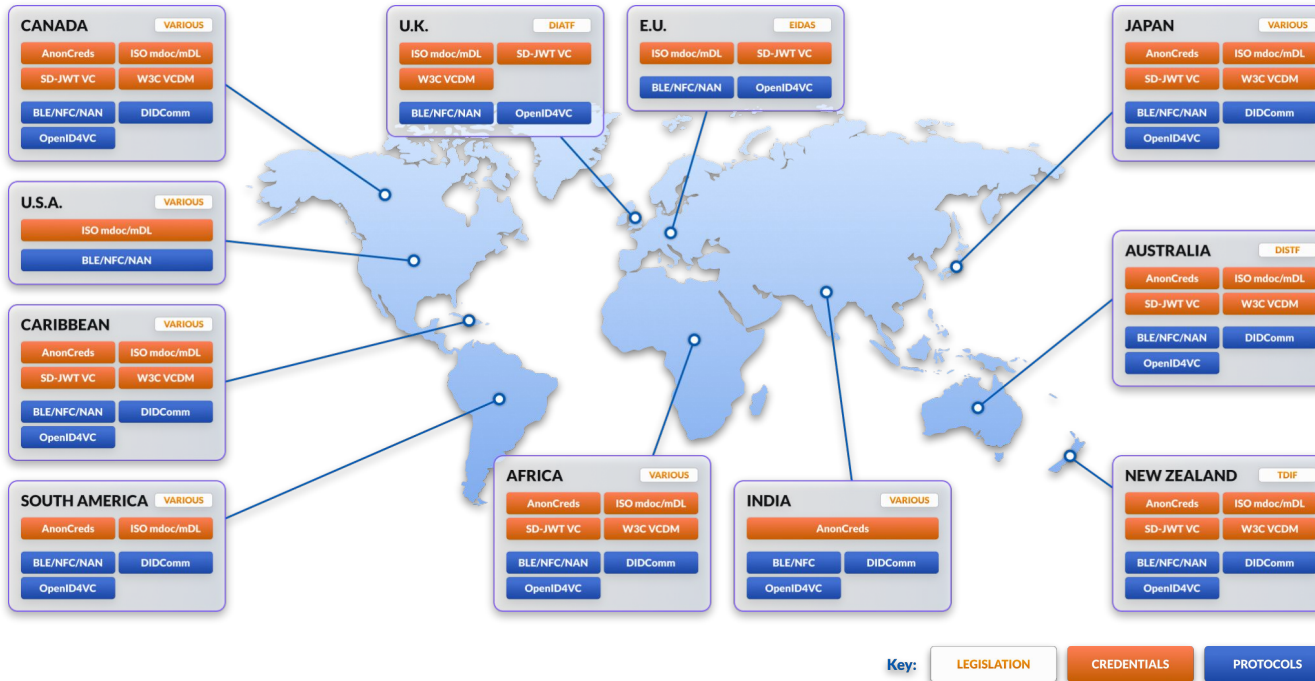


Indicio has you covered with a **white-label, multi-credential, globally interoperable, digital wallet — Holdr**

We've also got a **mobile SDK with all the needed code to add Verifiable Credentials to your existing digital apps.**



Where Indicio Proven can take you



Indicio makes global standards and cross-jurisdictional integration possible.

Entra, mdoc/mDL, EUDI, ICAO DTC-type credentials all work together on one platform, worldwide.

How to implement Indicio Proven

1. Sign a Proven license agreement.
2. Install Proven software in cloud or on-prem with help from Indicio.
3. Install Proven digital wallet or mobile SDK.
4. Add optional partner integrations, e.g. Regula IDV / biometrics.
5. Buy a transaction bundle (i.e., how many credentials do you want to issue/verify).
6. Add optional certified training from Indicio Academy. Courses cover all the business and technical aspects of decentralized identity.
7. That's it — unless you want customization.



And here's our recommended implementation roadmap.

Phase 1 – Prove it fast

For newcomers or organizations with a clear use case. A proof of concept can be completed on your timeline, using hosted components, digital wallet access, and hands-on training through Indicio Academy. This phase validates how credentials work in your environment and measures immediate efficiency gains.

Recommendation: don't waste time agonizing over which credential format to use. Just pick the one that best fits your business needs. Interoperability ensures you can consume and even issue other credential formats as your business use case requires.

Phase 2 – Expand and demonstrate ROI

For organizations ready to go beyond pilot. Adoption can expand with the mobile SDK, allowing credentials to be embedded in existing apps. Optional document authentication and biometrics increase assurance. The system is flexible to run on-prem, in the cloud, or as a hosted service. At this stage, you have the evidence to show cost savings, smoother workflows, and stronger fraud prevention across multiple channels.



Phase 3 – Scale and lead

For organizations ready for full production. This stage includes high-volume licensing, integration support, and ongoing services to manage millions of credentials. Document authentication and biometric options add assurance at scale. The result is transformative efficiency, lower operating costs, and digital interactions built on trust.

AI is both an existential threat and an opportunity. You know the stats and the risks. Indicio Proven's class-leading decentralized identity technology enables you to master both while focusing on the opportunities outlined in this paper.

You know what digitally-native consumers expect from technology. You see the trend towards automated, autonomous systems. So start now by starting small with Proven, see results quickly, and scale up when you're ready.

The payoff is faster onboarding, stronger fraud prevention, easier compliance, and better experiences for the people who matter most — your customers, employees, and partners.

Your digital future starts here:

Sales@Indicio.tech

[Join our mailing list](#)

[Get a free demo](#)

Copyright © 2026 Indicio PBC and/or its affiliates. All rights reserved.

Indicio trademarks and trade dress may not be used in connection with any product or service that is not Indicio's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Indicio. All other trademarks not owned by Indicio are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Indicio.

