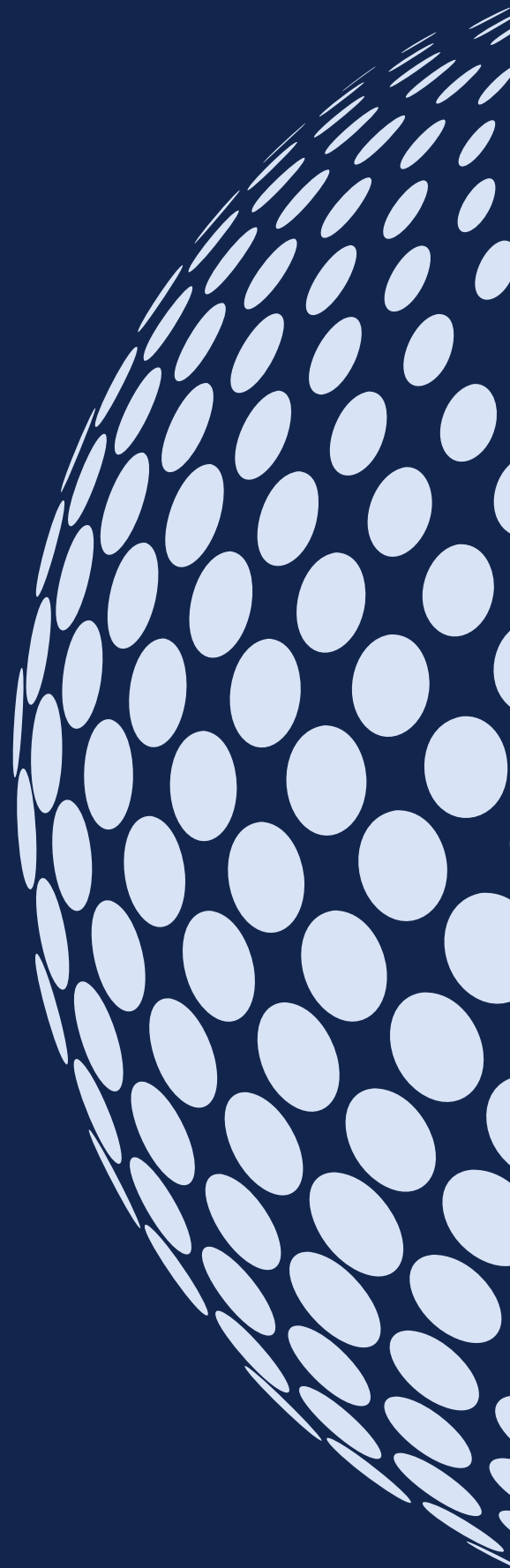




The Business Value of Interoperable Verifiable Credentials



Exec Summary

Decentralized identity and Verifiable Credentials address an overlapping set of operational, security, and compliance challenges around digital interaction, digital identity, and data sharing.

But these technologies are not only a solution to these problems, they also provide opportunities to scale trust, create Digital Public Infrastructure, and enable new kinds of digital interactions — provided they are implemented in an interoperable way following open standards.

Challenges

AUTHENTICATION AND INTEGRATION

The cost of authenticating user identity and data in the face of continuous identity fraud and data breaches.

The friction created from centralized methods of authenticating user identity and data, both on the back end, in terms of direct integrations, and on the front end through user-unfriendly multi-factor authentication.

The cost and complexities of creating direct integrations between disparate systems to share data.

SYSTEMIC RISKS FROM CENTRALIZED PERSONAL DATA

Consumer and political concern over privacy and especially biometric privacy, with market surveys showing that consumers would be more willing to use biometrics if their rights and privacy are protected.

The existential risk to consumers of biometric data breaches: you can reset a password, you can't reset a face.

The regulatory compliance burden of storing personal data, especially biometric data, particularly as the EU Digital Wallet mandate takes effect in 2026.

Opportunities

USER EXPERIENCE

Meet the expectations of digitally native users and consumers that digital interaction should be simple, seamless, and instant.

Foster social trust through consent and data privacy.

DRIVE DIGITAL EVOLUTION THROUGH PORTABLE TRUST

Facilitate expansion of digital identity to devices, digital objects, chatbots, and AI agents and address the exponential security risks and compliance burdens.

Facilitate agentic AI by providing secure, decentralized agent, customer, and user identities and permissioned data access so that AI can achieve its goals.

Scale Digital Public Infrastructure to support business growth and integration using low cost open source and open standards technology backstopped by digital identity assurance.

Support access to traditionally excluded populations in financial and government services.

Facilitate new kinds of trust networks, where integration and scale are made possible by instantly actionable data and trusted identities (e.g., decentralized finance).

Create a single, seamless market through instant, portable, trusted identity and data.

The challenges impose significant costs on business. They limit the speed and scale at which information can be authenticated and acted upon and impose a drag on market efficiency, scalability, and innovation.

The opportunities are central to the evolution of digital interaction, whether it is meeting fundamental authentication requirements or providing the consent and privacy protection that makes regulation easily manageable.

The ability to scale trust by removing uncertainty around identity and data is an economic multiplier, simplifying market interactions and facilitating innovation. In effect, decentralized identity and Verifiable Credentials enable the rapid creation of “trust rails” for interaction and transaction from anywhere to everywhere; they can scale rapidly across industries, sectors, and existing markets to create new kinds of trust networks. To access trust at these scales is its own source of innovation.

The underlying ability to trust the integrity of the information in the credential and to determine where that information has come from enables processes that would otherwise be costly, operationally impractical, at risk of error and fraud, and challenging in terms of compliance with data privacy regulations. Decentralized identity and Verifiable Credentials solve these challenges and create these opportunities by making data portability and provability inexpensive, simple to implement within existing systems, and, depending on the use case, rapidly deployable.

The best way to think about the business of decentralized identity is to understand how and why it is being deployed

With Gartner Research describing decentralized identity as delivering “magnitudes of improvement in terms of efficiency, cost and assurance” compared to “real-world” identity verification, this technology is highly disruptive to existing identity and access management approaches, while providing a much broader range of features to scale trusted digital identities and data sharing.

For example, Verifiable Credential technology combined with biometrics enables rapid scaling in security while simplifying implementation and compliance. This is because an authenticated biometric in a Verifiable Credential can be automatically compared with a liveness check without the verifying party having to store the person’s biometric data.

The ability of a person to carry a tamper-proof copy of their biometrics in a Verifiable Credential provides a simple solution for biometric identity fraud and AI-generated deepfakes as the person can corroborate a liveness check with a digitally-signed copy of their biometrics.

Remote onboarding, call-center fraud, and the strong assurance for payments are immediate applications where Verifiable Credentials with authenticated biometrics can reduce costs, mitigate risks, and scale innovation.

Similarly, as the market focuses on the capacity of agentic AI to use personal data to perform concierge-like customer services, the need for agents and customers to seamlessly authenticate each other and request and grant data access are critical to effective deployment.

This is not simply a matter of managing the recent explosion in AI-focused regulation: data privacy regulations such as the European Union’s General Data Protection Regulation (GDPR) constrain agentic AI through mandates on data and purpose minimization and consent.

Decentralized identity provides a **highly efficient architecture for intelligible interaction between digital identities** that can address the existing bottlenecks, costs, and risks around identity and data authentication and provide a foundation for new technologies to deliver the seamless benefits they promise as they expand in complexity.

1

No need to store data to prove it:

Information can be instantly verified, so there's no need to store it just for cross-checking during authentication. This lowers the cost of validating data and makes it easier to meet privacy and security regulations.

2

Information is easily portable

so that it can be shared between disparate databases and systems. This eliminates the need for expensive, custom direct integrations.

3

Act on data immediately: Because the information is already trusted, systems can use it right away. This means seamless operations and processes without any tradeoff in security.

4

Low cost of trust:

Information is disintermediated from third-party identity and access management systems and service brokers; market interaction can be streamlined, increasing profitability, especially to low-margin businesses.

5

Data privacy and protection compliance is easier:

People, organizations, devices, chatbots and AI agents can have permanent, portable digital identities, hold data associated with these identities, and consent to sharing that data (or ask permission for access).

6

Biometric data can be cryptographically verifiable:

Biometric data can be verified through cryptography instead of needing to be cross checked with a copy of that data stored in a database. This prevents biometric identity fraud and generative AI deepfakes, and enables storage-less biometric authentication in compliance with EU biometric data regulations.

7

Information and trust can be easily orchestrated:

Rules about who can issue and verify credentials, and how information should be shared, are published as machine-readable files and propagated to every participant in a credential ecosystem.

These rules can be easily configured to manage complex workflows or use cases where there are different, hierarchically arranged authorities (such as airspace). As the rules are cached in each user's software, everyone in the system follows the same set of rules, and verification is possible in offline situations via BLE or NFC.



Five Verifiable Credential Use Cases

Any business activity or social interaction that requires proof of identity or verified information can benefit from decentralized identity and Verifiable Credentials. This is because the technology is not just another identity tool; it is a foundational approach to how digital information is created, shared, and trusted.



Because this technology can be applied to almost every aspect of private and public sector activity, it can be difficult to see where exactly you can start deploying it. The following use cases overlap and are by no means exhaustive, but they capture the practical benefits of this technology. They also articulate the kinds of opportunities that arise from scaling a trust-based architecture using interoperable systems rather than simply implementing a shinier identity verification product.

1 Quickly enable efficient backend operations, seamless front-end processes

Seamless efficiency follows from verifiability: If you trust the issuer of the credential, you can trust the data in the credential. This is because the data has been digitally signed, and any attempt to change the data is immediately detectable. Adding authenticated biometrics and identity and device binding, creates multi-dimensional ways to establish trust.

This kind of portable trust means data can be immediately consumed and acted on, reducing the cost and friction of normal authentication processes and eliminating the need for direct integrations between disparate systems. Portable trust also reduces the risk of fraud, the cost of authentication and the cost of security.

For the consumer, customer, or user access to accounts is seamless. They can access accounts or services by scanning a QR code, or clicking a link to present a credential. There's no need to remember logins, use passwords, complete multifactor authentication, or manually enter data.

And for the kind of identity authentication needed for KYC, payments, and travel, the ability to hold an authenticated biometric in a Verifiable Credential means that a person carries a back up proof of who they really are that can be verified without a relying party — like a bank call center — having to store their biometric data. This provides a powerful way to mitigate the rapid increase in biometric identity fraud, generative AI deepfakes, and the general escalation in AI-mediated identity fraud.

2 Scale trust, extend identity, create markets

When you can trust both identity and the data tied to it, you unlock new ways to build secure, efficient, and privacy-respecting systems. This trust foundation makes it possible to scale services, expand access, and create new market opportunities.

Trusted identity and data means that:

People can have seamless digital experiences that are both secure and privacy-preserving, without needing to sacrifice one for the other.

Interoperability through governance makes it possible for Verifiable Credentials to scale globally and connect disparate ecosystems and credential types.

Trust can move between systems and organizations, making it possible to create new products, services, and markets.

People lacking formal identity can gain access to secure, permanent, portable identities helping them participate in the economy and society.

Devices can be given secure digital identities and managed through governance rules that control how they interact and share data.

AI agents can use secure digital identities to authenticate and act on behalf of individuals, with the user's permission to access and use their data.

We think of market efficiency in terms of prices reflecting all available information and reducing the possibility of arbitrage. By being able to price trust through Verifiable Credentials, we reduce the risk of arbitrage through uncertainty — in this case, fraud. The participants in a market and the information they share are fully intelligible to each other, enabling markets to develop and grow, especially in otherwise low-trust environments.

This is one of the reasons why decentralized identity is being used to build digital public infrastructure.

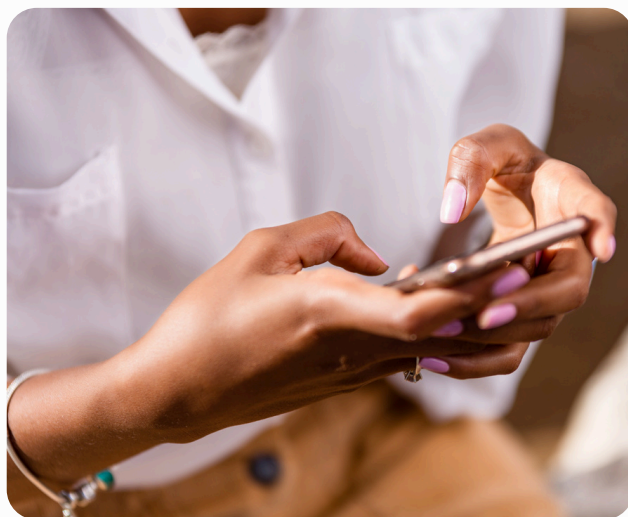
3 Create “government grade” digital identities using authenticated biometrics

By incorporating authenticated biometrics and validated passport data into a Verifiable Credential (following global standards set by the International Civil Aviation Organization), you can create a digital equivalent of a passport, bind it to its legitimate owner and their device, and verify it instantly, anywhere — without having to check in with the original source of the data or store biometrics to verify the authenticity of the credential.



The combination of biometrics, identity binding, tamper-proof data and cryptography enable the strongest possible digital assurance of identity.

This data is held in a digital wallet on a mobile device (or cloud-hosted wallet) and enables fully portable data sharing, with the capacity for offline verification.



And with the holder bringing their own data and biometrics, complying with data privacy regulations around consent, portability, and data and purpose minimization is radically simplified.

Seamless data sharing and authentication with government-grade digital identity makes critical and high value digital interactions easy and immediate, such as border crossing, account authentication, and payments.

4 Protect against deepfakes

Authenticated biometrics in a Verifiable Credential also provide a way to mitigate biometric identity fraud, account takeovers, and generative AI deepfakes.

With an authenticated biometric either derived from a valid passport chip (and verified with a liveness check) or created during a specific identity assurance process, a person can be instantly cross checked during by presenting their biometric credential when they submit to a liveness check.



If the digitally-signed template in the credential resolves to show it has not been altered and matches the person's live biometric scan, access can be granted.

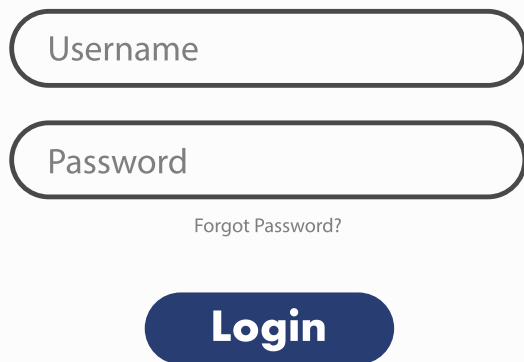
This bypasses the growing threat of biometric identity fraud and deepfakes. It transforms remote authentication and call center account management.

And authenticated biometrics can be combined with other contextually relevant data, either in the credential itself or from other credentials. It is possible to cryptographically prove that the person issued with an authenticated biometric credential has also been issued with other credentials.

5 Avoid storing personal data in centralized repositories

Centralized data, especially personal data, is at permanent risk of being stolen. As of June 2025, the scale of data breaches can only be described as ridiculous.

According to Cybernews, its research team has estimated that **16 billion login credentials** were stolen from 30 databases since the beginning of the year, with the data breach affecting all the major tech companies.



There is no need to keep doing this — or relying on identity providers who do this.

Decentralized identity and Verifiable Credentials enable people, organizations, and devices to hold their own identity data in a secure way and present that data for verification without the verifying party needing to cross check it against stored data.

This is the only way forward.

You can begin this journey by switching to use a Verifiable Credential for single-sign on.

This is an ideal solution for small and medium enterprises as it enables a substantial increase in security with the bonus of access management and orchestration built in at low cost. It is then comparatively easy to extend credential uses to other critical data sharing and authentication operations.

2026 — Are you ready?

The European Union's mandates around digital identity (eIDAS) and digital wallets (EUDI) are creating a single digital market for its 450 million citizens.

To do business in this market requires adopting decentralized digital identity and Verifiable Credential technology and thinking strategically about how to gain market share, interoperate, and drive innovation as quickly as possible.

The clock is ticking.

The European Commission has mandated that every member state make an **interoperable digital wallet** for digital identity through Verifiable Credentials available to all citizens, residents, and businesses **by 2026**.

At the same time, the efficiency argument for decentralized identity is driving the development of Digital Public Infrastructure in Africa and Asia.

In India, hundreds of thousands of sole traders and SMEs can integrate and create markets and avail of financial services through digital infrastructure that makes identity and data provable.



And — this is critical — everyone wants to interoperate. EUDI doesn't just mean a single digital market for Europe, interoperability means a single digital market for the world.

This is why decentralized identity is not just another identity and access management product: It's a foundation for building a more efficient and inclusive global internet; it's a digital architecture for trust.

To Europe and the world with Indicio Proven®

In this rapidly emerging marketplace for digital trust, Indicio has created **Indicio Proven** as a complete system for deploying the widest possible range of decentralized identity and Verifiable Credential formats, protocols, and supporting infrastructure.

Proven allows businesses to rapidly implement solutions that best address their specific use cases while maintaining global interoperability.



What you can do with Proven

Interoperate and move seamlessly between EU and global digital identity and wallet specifications.

Create multi-credential, multi-protocol workflows that bridge credential formats for simple user workflows.

Conduct tens of thousands of credential verifications simultaneously with the most powerful, most robust mediation software in the market.

Create “government-grade” digital identities for Digital Passport Credentials that follow International Civil Aviation Organization specifications for Digital Travel Credentials (DTC).

Combine DTC and EU-specified credentials in a single workflow for international travel.

Derive Verifiable Credentials from paper documents or plastic cards.

Deploy credentials for eVisas and electronic travel authorization.

Conduct document, face match, and liveness checks for financial KYC and issue as credentials.

Use Verifiable Credentials for issuing business licenses, certifications, course transcripts, diplomas and degrees, and qualifications of any sort through the Open Badges 3.0 format.

Choose from Deploy AnonCreds, SD JWT VC, mdoc/mDL, AnonCreds, and Open Badges 3.0 credentials; OID4VC and DIDComm; BLE, NFC, and Wifi Aware.

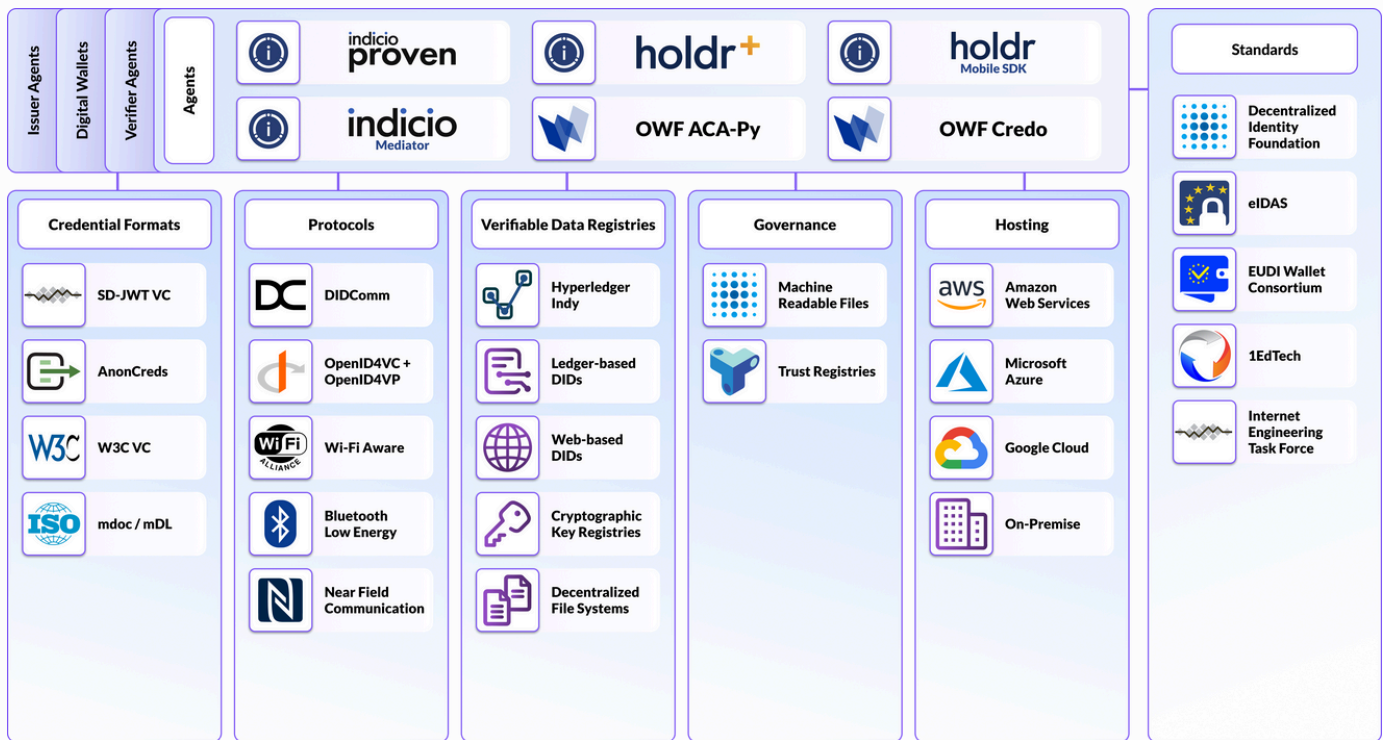
Easily add Verifiable Credentials to existing Android and iOS apps using the Holdr+ Mobile SDK.

Use a white-label globally-compatible digital wallet.

Easily implement decentralized governance and trust lists following the Decentralized Identity Foundation's Credential Trust Establishment specification; this facilitates interoperability and allows credential ecosystems to easily scale.

*"When we saw the work that **Indicio** has been doing with **biometric authentication** and **tamper-proof digital credentials** in travel, not only did we want to invest immediately in their main business, but we also recognized that their tech is shockingly translatable to the finance industry."*

Elijah Levine, CEO of BMIG.



Use Verifiable Credentials for issuing business licenses, certifications, course transcripts, diplomas and degrees, and qualifications of any sort through the Open Badges 3.0 format.

Choose from SD JWT VC, mdoc/mDL, AnonCreds, and Open Badges 3.0 credentials; OID4VC and DIDComm; BLE, NFC, and Wifi Aware.

Easily add Verifiable Credentials to existing Android and iOS apps using the Holdr+ Mobile SDK or use a white-label or other globally-compatible digital wallet.

Easily implement decentralized governance and trust lists following the Decentralized Identity Foundation's Credential Trust Establishment specification; this facilitates interoperability and allows credential ecosystems to easily scale.

© 2025 Indicio.tech. All rights reserved. This material includes original content created by Indicio and is protected under copyright. It may not be reproduced, adapted, or distributed in any form without prior written permission from Indicio. The content reflects the expertise and perspective of Indicio's team and is intended for informational purposes only. This material may not be used in the training, development, or refinement of artificial intelligence, machine learning systems, or related technologies. Use of this content is subject to Indicio's terms and conditions.

indicio
Let's Talk

Learn more at Indicio.tech

Contact US

Copyright © Indicio 2025. All Rights Reserved