indicio

A Verifiable Credential Is Much More Than A Digital Credential That's Verifiable

There are verifiable credentials. And then there are Verifiable Credentials. How do you know if you're buying a problem instead of a solution?

Introduction

Many ID providers offer “digital credentials” for use on mobile devices; some say ‘verifiable’ on them and some say that they are “decentralized.”

Spoiler, these are, almost certainly, not “Verifiable Credentials.”

Why is this distinction important?

A digital credential that makes an API call to a server for verification requires cross checking the information in the credential with the information stored on that server in a database.

A Verifiable Credential can be verified without having to make an API call to a server and database. Instead, the source of the credential is cryptographically verified and the integrity of the information is cryptographically verified as unaltered.

Introduction

Many ID providers offer **“digital credentials”** for use on mobile devices; some say ‘verifiable’ on them and some say that they are “decentralized.”

Spoiler, these are, almost certainly, not “Verifiable Credentials.”

Why is this distinction important?

A digital credential that makes an API call to a server for verification requires cross checking the information in the credential with the information stored on that server in a database.

A Verifiable Credential can be verified without having to make an API call to a server and database. Instead, the source of the credential is cryptographically verified and the integrity of the information is cryptographically verified as unaltered.

This verification doesn’t require storing the information to cross check it. Anyone verifying a Verifiable Credential just needs access to a small set of metadata to perform the cryptography, and this metadata is stored on a Verifiable Data Registry, which is either ledger based or web based. There’s also a way to verify without being online.

Not having to store personal data solves a critical security weakness of the internet era: data breaches and identity theft.

This also means that a Verifiable Credential can be verified independently, without needing to contact the original issuer. If the credential stops working when the issuer goes offline or ceases business, that means it does not meet the standard definition of a Verifiable Credential.

How to know you are getting a real Verifiable Credential?

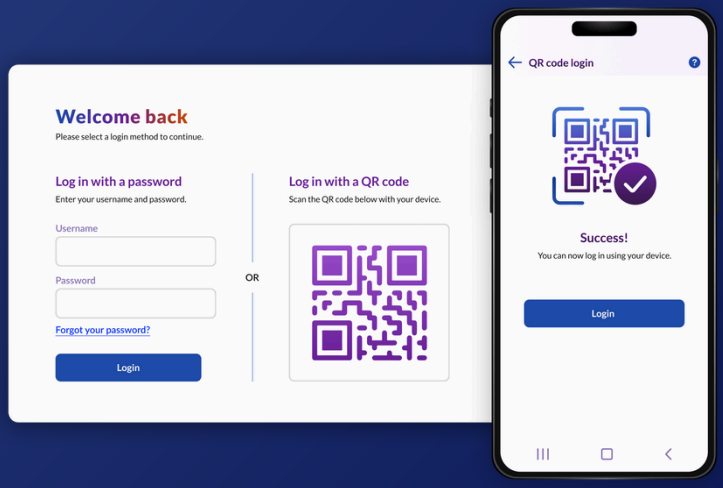
Think of Verifiable Credentials as being like a digital container system that can seal different types of digital information, such as the personal data and biometrics that constitute an identity or account information.

The container, meaning the Verifiable Credential, has **two essential properties:**

- You can always prove its origin
- You can prove that the contents of the container haven't been altered

When you can determine these two things, you can make a judgment call: Do I trust the original issuer of the credential? If I do, I can trust the contents by instantly performing cryptography to check the seal.

This ability, to verify both the issuer and the integrity of the data without contacting a third-party, is the fundamental difference between Verifiable Credentials and plain credentials.



The Value of Verifiable Credentials Over Plain Verifiable Credentials

No centralized data storage

We've already mentioned that not having to store personal to verify a digital identity for access to a resource solves one of the key security weaknesses in identity and access management. If you don't have to store high-value information, there's no high-value information to steal.

Identity, biometric and device binding

At the same time, a Verifiable Credential can't be shared or stolen or faked. It's cryptographically bound to the issuer and holder and biometrically bound and code restricted to the holder and their digital wallet. With the addition of an authenticated biometric to the Verifiable Credential, a liveness check can be cross checked with a Verifiable Credential presentation, which mitigated biometric identity fraud and deepfakes.

Biometric privacy and security

In doing all this, Verifiable Credentials also simplify data privacy compliance. Consider biometric data. When you add authenticated biometric data to a Verifiable Credential (either derived from the biometric data in a passport chip and compared with a liveness check or through direct identity assurance that captures a template), you don't have to store biometric data in order to verify it.

This has a huge value prop for businesses given the existential risks of biometric identity fraud (and if you are dealing with EU citizens, stringent biometric privacy regulation).

Access management, governance, offline verification

You can also easily configure governance rules for Verifiable Credentials that enable policy-based access. Machine-readable files sent to all the participants in a credential use case (issuers, holders, verifiers) establish which credentials are to be trusted, how those credentials are to be interpreted when presented, and who is a legitimate verifier. This enables granular access control for implementing least-privilage access to resources. And unlike passkeys, a credential holder doesn't have to be enrolled to be verified.

As these machine-readable files are cached in the software of each participant, offline verification is possible using BLE and NFC.

Simple to issue, simple to hold, simple to verify, and powerful to use — only if it's a Verifiable Credential.

When decentralized is actually centralized under the hood

"Decentralized" is another feature where the delta between branding and reality is large.

Verifiable Credentials work in tandem with decentralized identifiers (DIDs), which are unique, cryptographically verifiable identifiers created and controlled by the user. DIDs let two parties securely authenticate and communicate directly with one another, so they can issue, share, and verify information, without needing a third party in the middle.

This is the decentralized part of the value proposition. With DIDs, there's no need to rely on a certificate authority to prove identity. Instead, anyone can issue any number of DIDs from a digital wallet and prove that they control each of their DIDs.

But who exactly is in control of those DIDs? This is where Verifiable Credentials come in by adding the missing context. If someone presents a Verifiable Credential issued by a trusted source, like a passport office, you now know who is behind that DID. You can verify the identity of the person or organization or device or chatbot and also trust the communication channel they're using.

Go decentralized because you don't need to phone home anymore

You can see why conventional identity providers claim to offer "verifiable credentials and decentralization." The real thing completely upends their business model by being cheaper, faster, privacy-preserving, and much more secure.

Trustable information can now move from anywhere to anywhere without third party brokers or direct integrations between databases, and be instantly acted on, creating a seamless world.

Decentralized identity brings a myriad of benefits to existing identity systems.

- It's efficient — a really efficient way to interact digitally and conduct transactions.
- Identity assurance is baked in, with each party controlling their DID and their Verifiable Credential
- You no longer need third-parties to manage and validate the exchange of information.
- Trust is completely portable.
- Communication is peer-to-peer, but only after each party has mutually authenticated each other.

Of course, there is some digital infrastructure needed to support this — a Verifiable Data Registry for finding the issuer of a credential and the cryptographic keys to verify it. These registries exist on a distributed ledger, which provides long-term reliability, (for resilience and persistence) or simply on the web.

Either way, we are, again, leveraging efficiency: a million credentials can be issued from a single write.

Most importantly, this setup gives you permanent control of your identity and your data. It also doesn't rely on a third party to exist and it can't be taken away.

With plain "verifiable" credentials, that's not the case. You're "**renting**" identity, and must meet their terms. **The "credential" on your phone is just a fancy pointer to a backend database.** You're not in control — the identity provider is. And they're charging you for the privilege.

How to know you are buying an actual verifiable credential solution rather than a centralized solution marketed to look like something it's not

To summarize, here are the **five key features** of a Verifiable Credential:

1. The data is digitally signed by the issuer and tamper proof making it impossible to alter without detection.
2. The data is verifiable without phoning home. The verifier doesn't need to connect to a server or check with the issuer.
3. It supports secure peer-to-peer communication protocols. You connect directly across a secure channel with credential issuers and verifiers, without third-party intermediaries required.
4. You, the holder, control your data. Nothing is shared without your consent. Just like a plastic card in your wallet, you decide when to present it and to whom. use it when and how you want.
5. You, the holder, can selectively share data and use zero-knowledge proofs to share only the specific information that's needed without revealing full details.

If any of this is missing—if the credential lives on someone else's server or needs to check in with the issuer each time—it's not a Verifiable Credential—it's a digital permission slip with an expiration date.

Indicio Proven is you're complete Verifiable Credential solution

With Verifiable Credentials, identity moves like money: you can use it anywhere, carry it yourself, and no third party needs to watch every transaction. The key difference is that Verifiable Credentials are much harder to fake than cash.

This is what Indicio has created: support for the widest possible range of Verifiable Credential formats and communication protocols, making them usable across the widest possible set of real-world scenarios.

Get in touch to schedule a demo or book a free workshop tailored to your use case. We'll show you how to improve efficiency, cut costs, and unlock new opportunities for products and services using Verifiable Credentials.

Once you have the real thing, you'll wonder how you ever trusted anything else.

Indicio is a global leader in digital identity, authenticated biometrics, and Verifiable Credential technology with scalable solutions that organizations can rapidly deploy for increased efficiency, better user experience, and reduced cost. Our award-winning enterprise solution, Indicio Proven®, offers the widest range of interoperable decentralized identity options for global deployments, from single sign-on to seamless border crossing as well as compatibility with the European Union's digital identity and wallet standards.

Learn more about how Indicio is using this technology to successfully transform education, finance, government, health, travel and tourism, and supply chains at indicio.tech.