Whitepaper

Verifiable digital credentials: Secure, reusable identity for the digital era

Learn about VDCs — how they work and why they matter

The future of digital identity is here.

In a world where AI blurs the lines between humans and bots, proving someone is real—and who they claim to be—has never been more critical. Businesses need faster, more secure, and privacy-conscious ways to onboard users, verify access, and manage identity across ecosystems. Verifiable digital credentials offer a new approach — built on open standards, cryptography, and user control.

What are verifiable digital credentials?

Verifiable digital credentials (VDCs) are reusable, cryptographically-signed credentials that prove something about a person — such as their identity, age, employment, or qualifications. They're tamper-resistant and issued directly to a user's digital wallet of choice. Unlike traditional identity checks that are one-time snapshots, VDCs can be reused, instantly verified at the moment of need, and remain under the user's control.

- Tamper-resistant
- Reusable
- Minimize data exposure (selective disclosure)
- Built on global open standards

Why now?

📈 Identity-related challenges intensify

Regulatory complexity, onboarding friction, and fraud are on the rise — just as customers expect faster and more secure experiences.

🔐 Government-led initiatives are accelerating

The EU's eIDAS 2.0 regulation mandates support wallet-based verifiable credentials by 2027. In the US, mobile driver's licenses are projected to reach over 100 million users by 2030, with reusable identity pilots already in motion.

🌐 Interoperable standards are reaching maturity

Open frameworks like W3C Verifiable Credentials and OpenID now support real-world adoption, allowing organizations to build solutions that work across ecosystems and avoid vendor lock-in.

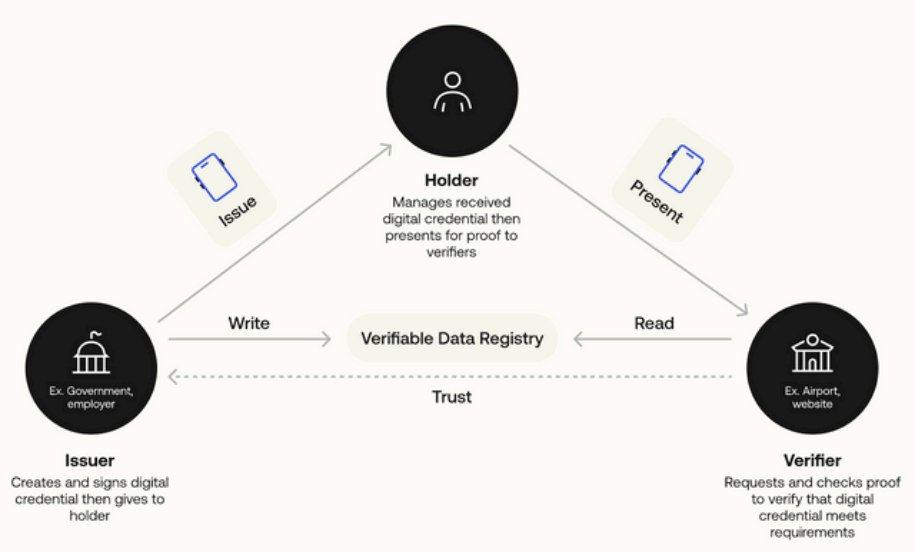
+100m

In the US, mobile driver's licenses are projected to reach over 100 million users by 2030.

How VDCs work

The basics

VDCs follow a simple, trusted pattern: an **issuer** (like a government agency, employer, or university) creates a credential that contains verified information that proves something about a person, signs it with their private key, and sends it to the person (aka **holder**)'s digital wallet.



When the person needs to prove something — such as their age or employment status — they present the credential to a **verifier**. The verifier checks the signature against the issuer's public key, instantly confirming authenticity without contacting the issuer or storing extra data. This cryptographic process makes verification fast, user-controlled, and minimizes unnecessary data sharing.

VDC use cases

How VDCs solve real world use cases

Customer onboarding — Verify identity, age, or eligibility instantly with mobile driver's licenses or trusted credentials — reducing abandonment, fraud, and manual review.

Workforce verification — Empower employees to prove their work-related credentials instantly (employers can issue a Work ID credential) — enabling secure account recovery, contractor onboarding, and partner collaboration.

Certification and compliance — Validate training, licenses, or achievements instantly — reducing certificate fraud and streamlining audits.

Benefits of VDCs

How VDCs can benefit your business

Lower verification costs	Eliminate costs and reuse trusted credentials instead of verifying from scratch each time.
Faster onboarding	Reduce friction by letting users verify with a digital credential — no document upload or waiting for manual review required.
Reduced risk	Reduce fraud and impersonation risks by replacing static documents with cryptographically signed credentials.
Enhance compliance	Minimize the amount of personal data you collect from users and stay compliant with GDPR and privacy regulations.

Getting started

Use cases in the real world

Begin with quick wins — such as adding mobile driver's license verification into your existing identity flow.

Okta will be integrating VDCs into existing Auth0 and Okta workflows to enhance what you're already doing. Plus, as the ecosystem grows, you'll be ready to support new types of credentials — from work IDs to certifications to partner-issued credentials.

Learn more and see VDCs in action — visit **oktacredentials.dev**