

Verifiable Digital Credentials

And How They Work



Summary

Verifiable digital credentials (VCs) are secure, digital versions of traditional identity documents, such as driver's licenses, issued by authoritative organizations like state DMVs, that provide validation of a specific claim about a person or entity. Unlike traditional paper or digital form factors of physical IDs, they can be independently validated in real time without relying on manual checks or verifying with centrally held databases. This makes them faster, more secure, and less susceptible to fraud.

Issued by trusted organizations (e.g. financial services, health services, schools, etc.), VCs allow the holder to control what information they share. For instance, a user can confirm they are over 18 without disclosing irrelevant [personal details](#) like their full birth date or home address. They contain the same identity information as their physical counterparts and can be stored in digital wallets on mobile devices, but the user is in control of which information is shared depending on the verification needed to access a particular service. VCs are designed to let users prove their identity online or in-person without needing to share unnecessary personal data or to physically present documents.

Benefits



Convenient

Streamline compliance for organizations and facilitate remote onboarding and access to services for individuals.



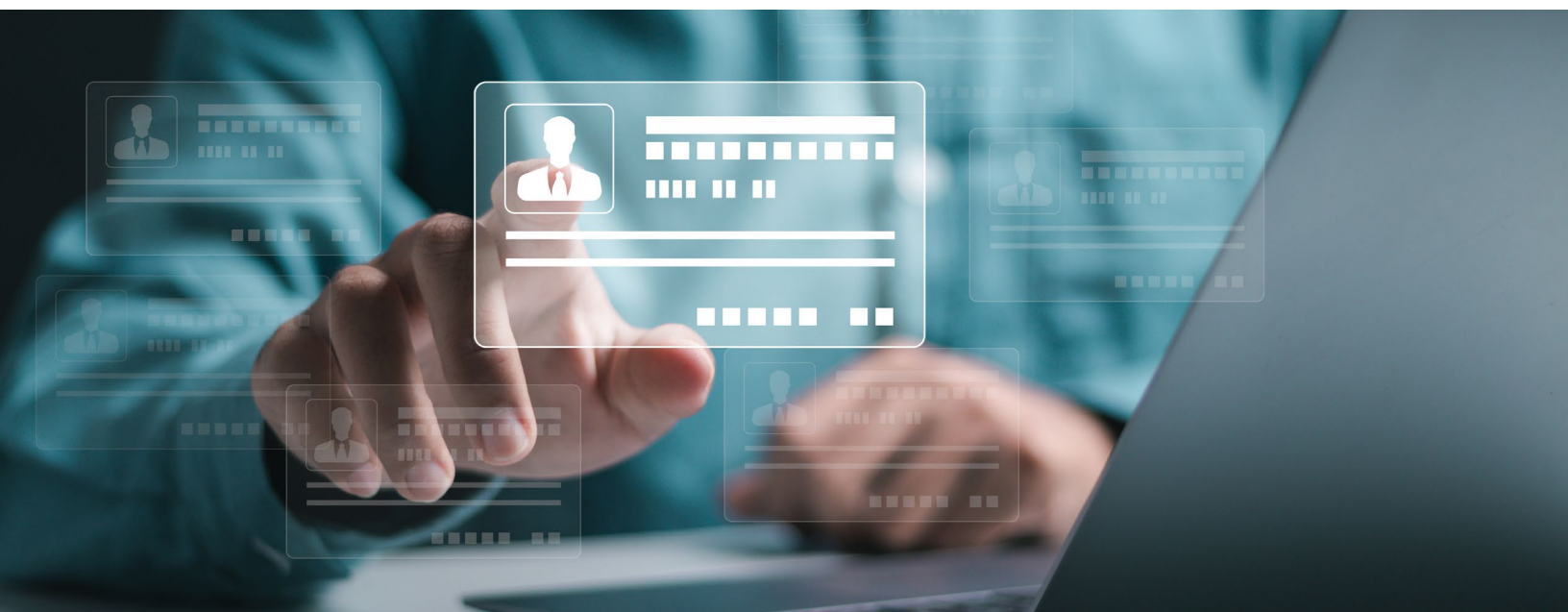
Privacy-protecting

Users can selectively share only the data necessary for a transaction, limiting unnecessary exposure of sensitive personal data and hence reducing risk of identity theft; verification takes place independently, without contacting the issuing authority so transactions can't be monitored.



Secure

Using secure digital wallets and biometric authentication ensures that only the rightful owner can access and present their credentials.



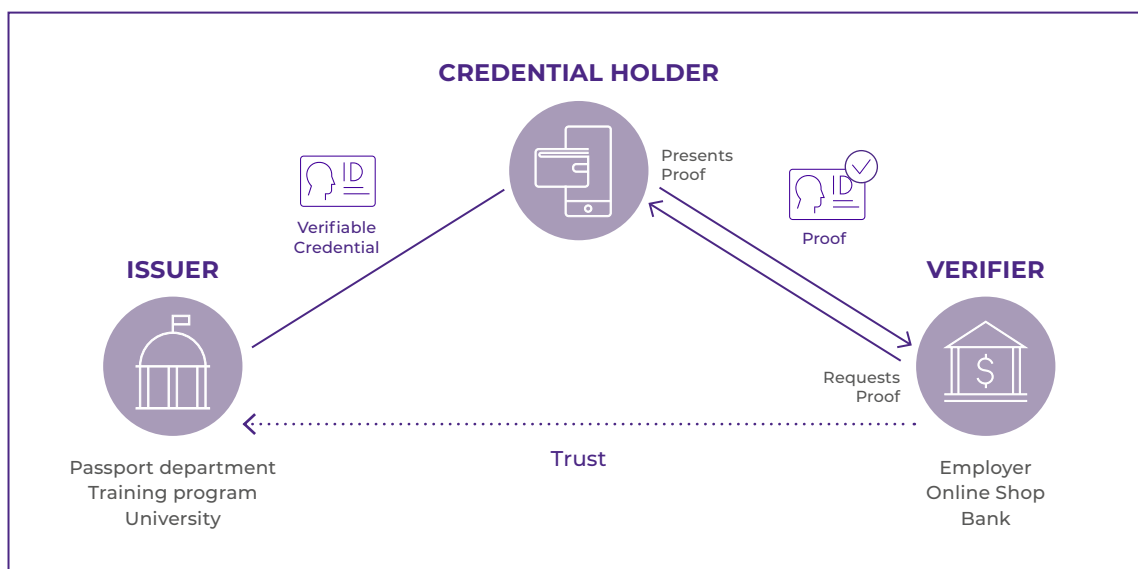
Verifiable	The ability to cryptographically verify the authenticity and integrity of the credential and information it contains.
Digital	Stored in a digital format, commonly in digital wallets on your smartphone – though may also be stored on cloud wallets in future. Designed to supplement the physical credentials you already use.
Credential	Statements about an individual, their identity, their status, and/or privileges. These can be government credentials (e.g., a driver's license or passport), education credentials (e.g., a diploma), or proof of certain personal attributes (e.g., age over 21).

Credit: [NIST](#)

When using a VC, such as a mobile driver's license, the process typically involves an issuer (e.g., a DMV) provisioning the credential to a digital wallet after verifying the user's identity. To access services—like opening a bank account—the user presents their V=C through their wallet app, sharing the credential with the relying party (e.g., the bank) for authentication. The relying party verifies the credential using a special code (or “key”) obtained from a trust service to

cryptographically verify the ID is authentic, without contacting the issuer directly and without any personally identifiable information (PII) being revealed or exposed.

This ensures privacy, security, and convenience while enabling organizations to confirm identities and grant access to services efficiently and securely.



Advantage of Digital Identities as Verifiable Digital Credentials

Digital identities, such as verifiable digital credentials (VCs), offer significant advantages for highly regulated industries like banking, workforce enablement, and healthcare. By enabling secure, cryptographic verification of identity, these technologies streamline compliance with strict regulatory requirements while minimizing the exposure of sensitive personal information. Users can selectively share only the data necessary for a specific transaction, reducing risks related to identity theft and data misuse. Additionally,

VCs facilitate remote/online onboarding and access to services, increasing convenience for both service providers and individuals, while maintaining robust privacy protections and auditability. Overall, digital identities enhance security, efficiency, and privacy in environments where regulatory standards demand rigorous identity management. As online and web-native activities continue to grow, the use of VCs represents both a secure and an efficient user experience.

Privacy Protection and Benefits of Digitally Verifiable Credentials

Digitally verifiable credentials, such as mobile driver's licenses, enhance privacy by allowing users to prove their identity online without sharing unnecessary personal identifying information (PII) and without contacting the issuer, ensuring that the issuer does not learn where or when the credential is used.

This approach minimizes the exposure of sensitive data and reduces the risk of identity theft or misuse. Additionally, using secure

digital wallets and biometric authentication adds further protection, ensuring that only the rightful owner can access and present their credentials.

Overall, digitally verifiable credentials offer a **convenient and secure way to manage identity online** while giving individuals **greater control over their personal information**.

Applications



Identity as Infrastructure: IDEMIA Public Security x Microsoft

IDEMIA Public Security is collaborating with Microsoft to support its new Microsoft Entra Verified ID solution, now live on the [Microsoft Marketplace](#). Organizations can access IDEMIA's identity proofing platform and issue a verifiable credential that enables seamless access to services across the Microsoft Entra ecosystem, without needing a costly and time-consuming custom integration.



Financial Services

Banks and financial institutions can leverage verifiable digital credentials to meet their know your customer (KYC) and anti-money laundering (AML) compliance requirements, as the credentials are both fraud-resistant and auditable, complying with the highest international standards for deterministic identity verification (vs. a probabilistic approach). The credentials can be used to authorize high-value, high-risk transactions, providing clearer fraud signals and reducing bank exposure. Further, VCs can enable more efficient and cost-effective client onboarding and KYC-sharing by and between financial service providers.



International Workforce Enablement

Based on IDEMIA Public Security's extensive coverage of global identity document templates, immigration and workforce mobility providers can leverage IDEMIA's digital identity verification and biometric capabilities to expand to use cases such as hospitality and travel, work authorization and international worker mobility, refugee processing, and more.



For more information, contact
us at **info@ps-idemia.com**