

DigipassONE™ Verify



Adopt digital identity wallets without complexity and extend trusted identity across onboarding, authentication, and transactions. DigipassONE Verify enables organizations to issue and verify digital credentials through a single integration layer. It bridges fragmented wallet ecosystems, allowing you to scale digital credentials while aligning with evolving regulatory frameworks and compliance requirements.

Scaling digital credentials without integration complexity

Manual document uploads, selfie checks, and knowledge-based verification are costly, slow, and introduce friction that drives user drop-off. As digital identity wallets scale and eIDAS 2.0 accelerates adoption, the path to faster, more secure onboarding is clear. But fragmented wallet ecosystems and evolving trust frameworks and standards make it difficult to deploy digital credentials across onboarding and authentication without significant integration overhead.

DigipassONE Verify provides a unified integration layer to support digital credentials across onboarding, authentication, and transaction scenarios, connecting to multiple wallet ecosystems through a standards-based approach while enabling orchestration with policies and contextual signals. This reduces integration complexity, supports regulatory alignment, and enables consistent, low-friction user journeys, providing a scalable foundation for digital credential adoption within a broader authentication strategy.

From static identity to verified trust

Digital credentials replace scanned documents with cryptographically verifiable claims, presented directly from a user's wallet without oversharing sensitive data. DigipassONE Verify acts as both issuer and verifier, enabling organizations to request and validate attributes — such as identity, age, or account ownership — at the precise moment they're needed. This shifts identity assurance from a one-time onboarding event to a dynamic, continuously verifiable trust layer across the full customer lifecycle.

One platform for every authentication scenario

DigipassONE Verify integrates wallet-based credential flows alongside passkeys, MFA, and Strong Customer Authentication (SCA) within a



Highlights

- Global wallet ecosystem, single integration**
 Connect to digital identity wallets across regions and regulatory frameworks through a unified OpenID4VC-based connector.
- Frictionless identity verification**
 Replace manual checks and fragmented ID proofing with cryptographically verified credentials for faster onboarding, lower drop-off, and reduced cost.
- Flexible invocation across channels**
 Meet users where they are with wallet invocation via app links, and QR codes across mobile and web.
- Integrated with your authentication stack**
 Works within the DigipassONE platform to combine credential verification with adaptive SCA, passkeys, and fraud signals in a single policy layer.
- Enterprise-grade scale and integration**
 Proven at high transaction volumes with seamless integration into IAM platforms and enterprise applications.



single policy layer, combining device signals, risk context, and credential verification to make real-time access decisions. Native wallet invocation reduces authentication drop-off across mobile and web channels, while built-in WYSIWYS signing and trust framework connectivity keep organizations audit-ready as eIDAS 2.0 requirements take effect. Security and usability are no longer a trade-off.

Built for what comes next

Standards evolve. Wallet ecosystems shift. DigipassONE Verify is architected to absorb that change server-side. Customers integrate once and stay current without re-engineering their stack. Pre-built connectors and a single API compress deployment timelines from months to weeks. And as an active contributor to the FIDO Alliance and EU working groups, DigipassONE Verify is built to emerging standards before organizations are required to meet them. The result is more than a wallet connector, it is a complete authentication foundation for the digital credential era.

SUPPORTED ENVIRONMENTS		
Cloud platforms	• AWS, Microsoft Azure, Google Cloud Platform	
Operating systems	• Rocky Linux 9 and 10, Red Hat Enterprise Linux 9/10, Amazon Linux 2023	
Java	• Red Hat OpenJDK 17, 21, and 25 • Oracle JDK 21 and 25	• Eclipse Temurin JDK 17, 21, and 25 • Bouncy Castle Java FIPS 1.0.2.x
Application server	• Apache Tomcat 10.1 and later	
Databases	• Oracle 21c Enterprise, 23c • MySQL 8.4.x • PostgreSQL 15, 16, 17 • AWS Aurora/MySQL 8.0.x and AWS Aurora/PostgreSQL 17.6 • CockroachDB v23.2.x, v25.2.x	
Analytics	• Via DigipassONE Insights add-on	
Mobile & app SDK platforms	• Android 5.0+, Wear 2.0+ • iOS 14+, watchOS 4.2+ • JavaScript • Objective-C, C++, Swift, Cordova, Java, ReactJS	
App types	• Web Apps, Progressive Web Apps (PWA), Mobile Apps, Hybrid Apps using WebView or mobile browser via App Links/ Universal Links.	
Widgets	• Sign-in, Transaction approval, Sign-up, Credentials (customizable UI)	
Wallet types & protocols	• EUDI Wallets: Mobile Wallet, Cloud Wallet, local external HW, HW Wallets, Apple Wallet and Google Wallet • OpenID4VCI and OpenID4VP	



Key Features

- Adaptive policy engine**
Code-independent policies combine device, contextual, and third-party risk signals to support registration, onboarding, and authentication.
- Wallet ecosystem support**
 - EUDI Wallets
 - OpenID4VCI and OpenID4VP
 - App links, and QR code invocation
- Device and risk signals**
Combines device, network, behavioral biometrics, and third-party risk insights to strengthen fraud detection.
- Administration and lifecycle management**
Web console and CLI for policy management, import/export, and analytics with role-based access. Supports onboarding, recovery, suspension, and deprovisioning, with tamper-evident audit logs for compliance.
- Analytics & reporting**
Detailed app incidents via DigipassONE Insights add-on.
- Integration & extensibility**
REST APIs, JWT authorization, and plugin support. Out-of-the-box integration with Keycloak, ForgeRock Identity Platform, Microsoft Azure B2C, and PingFederate.
- Flexible deployment**
Deploy as SaaS or on-prem, across any environment.

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world’s 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Copyright© 2026 OneSpan North America Inc., all rights reserved. OneSpan®, the “O” logo, DigipassONE™, Cronto® are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners. This content is provided for informational purposes only and is provided “as is,” without warranty of any kind, whether express, implied, statutory, or otherwise, including without limitation warranties of merchantability, fitness for a particular purpose, or non-infringement. Product specifications, features, roadmaps, and availability are subject to change without notice and do not represent a commitment. OneSpan does not warrant that any specifications or performance characteristics described herein will be achieved in all operating environments. Last updated: July 2026.

Learn more at
[OneSpan.com/security](https://onespan.com/security)

Contact us at
[OneSpan.com/contact-us](https://onespan.com/contact-us)

