



Digipass[®] S3 Authentication Software v9.5

Simpler logins, stronger security—powered by passkeys and beyond.

Passwords remain one of the leading causes of breaches, driving up costs for organizations and frustration for users. Passkeys, based on FIDO (Fast Identity Online) standards, provide a stronger, simpler alternative by turning devices people already use into secure authenticators.

Digipass S3 Authentication Software helps organizations move beyond passwords with phishing-resistant passkeys, while also supporting a broad range of modern authentication methods including Digipass Quick Authentication, intelligent passwordless authentication, out-of-band methods, OTP, and Secure Payment Confirmation.

With adaptive policies, device and risk awareness, and deep integration with leading IAM platforms, the software ensures security and usability work together in real-world environments.

The portfolio includes:

- Digipass S3 Server
- Digipass S3 Mobile SDK (Android + iOS)
- Digipass S3 Web SDK

These are also available as a delivery option through Digipass S3 Cloud for organizations that prefer cloud-based deployment.

Enterprises can adopt passkeys and modern methods while continuing to leverage existing OTP and MFA solutions, giving them flexibility to modernize at their own pace and scale

Features

Adaptive rulesets

Code-independent policy supports registration and authentication. Policies can combine multiple signals, including SDK-generated signals, contextual information, and third-party risk data. Flexible sequences avoid unnecessary prompts (e.g., first-time device use, high-value transactions, or untrusted devices).

Authentication methods

- Passkeys and FIDO protocols (UAF, U2F, FIDO2/WebAuthn), including synced and device-bound passkeys
- Quick Authentication and Intelligent Passwordless Authentication
- Autofill, Conditional UI, Conditional Create, and custom authenticator names
- Attestation and FIDO Metadata Service support
- Out-of-band authentication (QR codes, push, app-less)
- Secure Payment Confirmation (SPC) and PSD2-SCA
- OTP (email, SMS) and ID verification through third-party services

Device & risk signals

Device health, model, type, manufacturer, OS version, SDK version, IP address, location, velocity, Wi-Fi network, device “on-call,” and friendly fraud detection. Supports contextual integration with third-party risk engines and behavioral biometrics.

Administration & lifecycle management

Commandline tools (CLI) and web-based console for policy management, import/export, and analytics. Role-based admin permissions.



Highlights

- **Intelligent passwordless authentication.** Adaptive, policy-driven controls dynamically adjust security based on authenticator strength and device context for unmatched flexibility and compliance.
- **Easy migration to passwordless.** Gradually adopt passkeys and modern methods while continuing to support existing methods like OTP and MFA.
- **Secure, frictionless access.** Prevent account takeover with phishing-resistant passkeys and passwordless login experiences that work seamlessly across devices, apps, and channels.
- **Fraud-aware protection.** Strengthen defenses with device health checks, contextual risk signals, and friendly-fraud detection, beyond credential security.
- **Enterprise-grade, scale & integration.** Proven to handle millions of authentications while integrating easily with IAM platforms and enterprise applications.

Supports onboarding, recovery, suspension, and deprovisioning with tamper-evident audit-logs for compliance

Analytics & reporting

- Detailed statistics on authentication adoption, device usage, transactions, and deregistrations via Smart Analytics add-on. Incident visibility via App IQ add-on.

Integration & extensibility

- REST APIs, JWT authorization, and plugin support (e.g., session management, crypto). Out-of-the-box integration with Keycloak, ForgeRock Identity Platform, Microsoft Azure B2C, and PingFederate.

Deployment options

- Cloud or on-premises deployment with container support (Docker, Kubernetes) and multi-tenancy. Available as FedRAMP High and DoD IL5 service (via UberEther).

Customer testimonial

“ Traditionally, one of the biggest challenges of authentication systems has been to balance security with user experience. Due to the FIDO standard, both elements work together seamlessly to provide the highest security standards, along with a transparent and agile user experience. ”

- Financial services executive

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
DevOps	• Docker and Kubernetes deployment support through Cloud Deployment Toolkit (CDT) • Red Hat UBI9 base image (custom OS images supported)
IoT support	• Via Smart Analytics and App IQ (licensed separately)
Mobile & app SDK platforms	• Android 5.0+, Wear 2.0+ • iOS 14+, watchOS 4.2+ • JavaScript with WebAuthn API • 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, Android Widgets with activity-less Silent Authentication
Widgets	• Sign-in, Transaction approval, Sign-up, Credentials (customizable UI)
Secure hardware	• Secure Elements, Trusted Execution Environments (TEE), Secure Enclave • Platform and roaming authenticators (security keys, passkeys, biometrics, PINs, FIDO-enabled banking cards) • Import of pre-provisioned credentials

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.

Learn more at OneSpan.com/security

Contact us at OneSpan.com/contact-us

