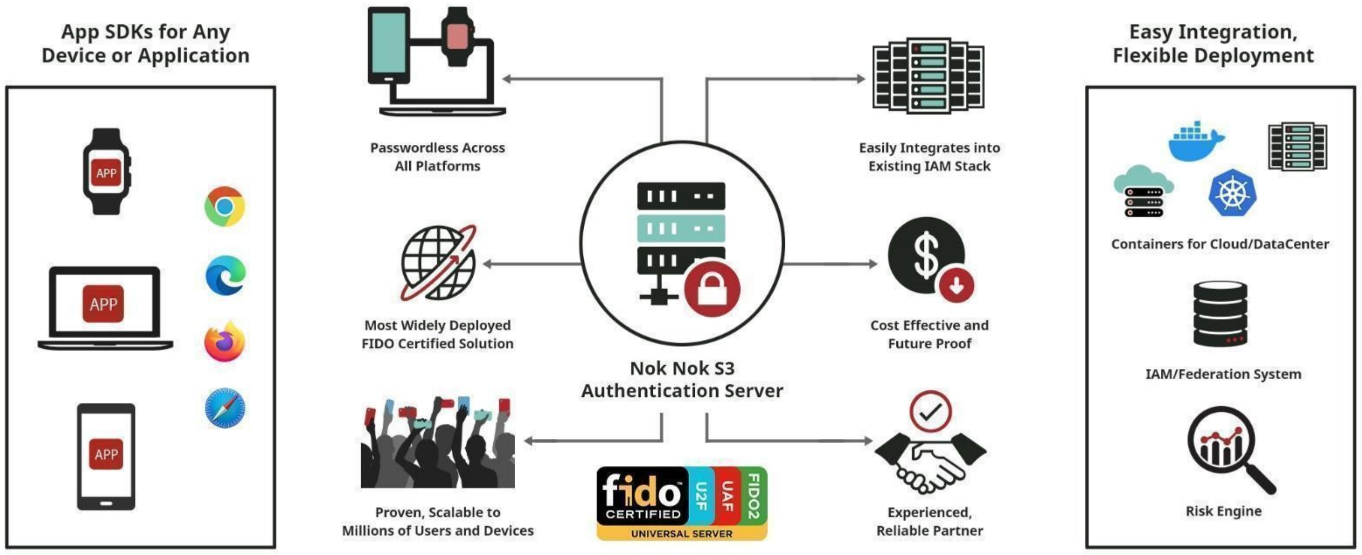
S3 Authentication Suite v9.0 Datasheet

DATASHEET

The Nok Nok^{TM} S3 Authentication Suite (S3 Suite) provides passwordless authentication that is significantly more user-friendly than legacy authentication and is more secure than traditional two-factor authentication, creating a vastly improved user experience and reduced account takeover.

The S3 Authentication Suite includes an Authentication Server and App SDKs for mobile, web and smartwatch applications. It leverages the security capabilities already present on a user's device to bring strong and convenient authentication to any application.

The S3 Suite enables organizations to easily turn user's devices into strong, multi-factor authenticators through support for all FIDO protocols, including passkeys. And, with the S3 Suite's rich set of capabilities, organizations can support the full customer lifecycle from frictionless on-boarding, progressive profiling, easy bootstrapping of new devices, account recovery, suspension and deprovisioning of users, to call center authentication support.


App SDKs for Any Device or Application
APP
APP
APP
Passwordless Across All Platforms
Easily Integrates into Existing IAM Stack
Most Widely Deployed FIDO Certified Solution
Cost Effective and Future Proof
Nok Nok S3 Authentication Server
Proven, Scalable to Millions of Users and Devices
fido CERTIFIED
U2F
UAF
FIDO2
UNIVERSAL SERVER
Experienced, Reliable Partner
Easy Integration, Flexible Deployment
Containers for Cloud/DataCenter
IAM/Federation System
Risk Engine

Find Out More

For more information about the Nok Nok S3 Authentication Suite, please visit https://noknok.com/products/s3-authentication-suite/. Nok Nok provides a variety of trial options for the S3 Authentication Suite including Software-as-a-Service, container image, and installable software. To try Nok Nok's solutions, please visit https://www.noknok.com/demonstration.

FEATURES	BENEFITS
Adaptive Rulesets	The S3 Suite Adaptive Rulesets provide code-independent policy support for registration and authentication. The policies can source multiple inputs including strong signals generated by the S3 Suite App SDKs, contextual information provided by business applications, and risk signals provided by 3rd party risk tools. In addition, it provides the flexibility to avoid additional authentication prompts (e.g., if last login is recent and risk is low), trigger authentication sequences (e.g., if transaction amount is high or a multi-device credential is used the first time on a device), or deny access (e.g., when a specific device is not trusted).
Authentication Protocols and Methods	FIDO UAF, FIDO U2F, FIDO2, WebAuthn - including synced passkeys, device-bound passkeys, DPK, attestation and FIDO Metadata Nok Nok^{TM} Quick Authentication, Nok Nok^{TM} Intelligent Passwordless Authentication and Nok Nok^{TM} Granular Adaptive Orchestration. Open ID Connect (OIDC) Federation Support Support for Suggestion of authenticator registration, Credential Sharing between Native and Web Applications, End-User preferred custom authenticator names Out of Band: QR-codes & push notifications. App-less Out of Band Authentication Support for PSD2-SCA, W3C Secure Payment Confirmation (SPC), 3DS2-delegated authentication and dynamic linking (non-repudiation) Email-OTP, SMS-OTP and Photo ID + Live Picture (Selfie) through third-party services
Device & Risk Signals	Device health, device model, device type, device manufacturer, device OS version, App SDK version, IP address, location, velocity, Wi-Fi network, Friendly Fraud and supports context data for easy integration with third party provided risk engines and behavioral biometrics systems.
Administration Console	Web-based UI for managing the Authentication Server. Allows administrators to configure policies, change properties, and review server analytics details.
Granular Administrator Permissions	Granular administrator permissions make it easy to apply least privileges to different operational roles, such as call center or help desk agents, business analysts, administrators, etc.
Multi-Tenancy Support	Serve multiple segregated user groups with authentication from a single authentication suite to improve operational efficiency.
Reporting and Analytics	View, generate, and download statistical data and authentication reports. Provides user base insights including unique users, device models, authenticators, authentications, transactions and deregistration over specified time periods. Tamper evident audit logs for compliance requirements.
Integration	Full server-side plugin support including session plugins, secrets store, and crypto integration. Customizable REST API, JWT authorization tokens, and EMVCo 3DS FIDO Data ("FIDO Blob"). Built-in connectors to ForgeRock® Identity Platform and PingFederate®. OpenID Connect (OIDC) support.
Authentication Server Supported Platforms	**Cloud platforms:** AWS, Microsoft Azure, Google Cloud Platform **Operating Systems**: RHEL 7, RHEL 8, CentOS 7, Red Hat UBI for Docker **Java**: Adoptium and Red Hat OpenJDK 11 and 17, Oracle JDK 11 and 17 **Application Server**: Apache Tomcat 9.0.32 or later **Databases**: Oracle 19c, Oracle 12c Release 1, MySQL 5.7.10+, PostgreSQL 9.2+ **DevOps**: Cloud deployment toolkit with Docker and Kubernetes support **IoT Support:** In combination with Nok Nok's IoT SDK (licensed separately), IoT SDK authenticates users to IoT devices
App SDK Supported Platforms	**Platforms**: Android 4.4+, Wear OS 7.1.1. API 25 and later, iOS 8+, watchOS 4.2 and later, JavaScript with WebAuthn API **Programming environments**: Objective-C, C++, Swift, Cordova for native Apps, Java, JavaScript **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 **Secure Hardware**: Secure Elements, Trusted Execution Environments (TEE), Secure Enclave **Authenticators**: FIDO2/WebAuthn platform authenticators and roaming authenticators ("Security Keys") supporting any modality, authenticators using native APIs (e.g., passkeys, Touch ID, Face ID, Android Biometric API, Android Keyguard), PIN/Passcode authenticator, user presence authenticator, silent authenticator, Phone as a roaming authenticator – CTAP2 "hybrid", 3rd party authenticator ASMs supporting any modality (e.g., speaker recognition), Class 2 biometric sensor support, FIDO authentication using Huawei Mobile Services, CTAP/NFC FIDO2 Payment Card Support

nok nok

ABOUT NOK NOK

Nok Nok lets you create safer, faster user experiences with key-based passwordless authentication based on the FIDO standards that enable compliance with global user and data privacy regulations. Nok Nok is the leader in passwordless customer authentication and is trusted by the biggest banks, telcos and fintechs including BBVA, Mastercard, Intuit, NTT DOCOMO, Standard Bank, T-Mobile, and Verizon. For more information, visit www.noknok.com.

Nok Nok Labs, Inc. 2890 Zanker Road, Suite 203 San Jose, CA 95134 USA