



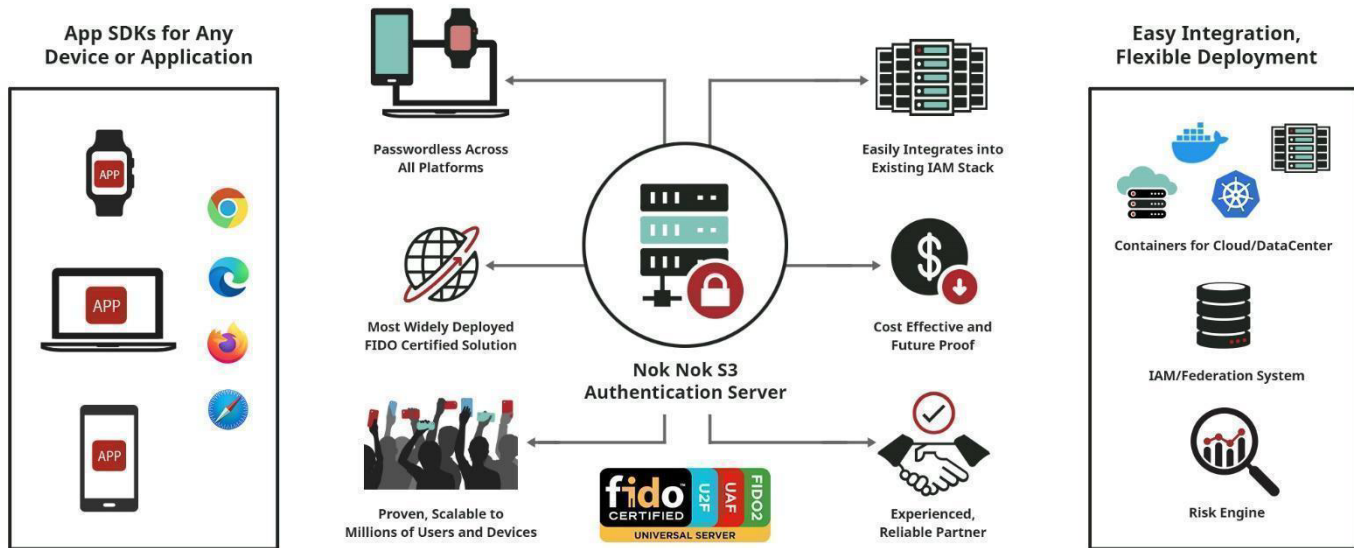
## S3 AUTHENTICATION SUITE V9.2 DATASHEET

DATASHEET

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

The S3 Suite includes an Authentication Server and App SDKs with Widgets 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 users' devices into strong, multi-factor authenticators through support for all FIDO protocols, including device-bound and synced 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, deprovisioning, and call center authentication support.



### 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
<b>Adaptive Rulesets</b>	<p>The S3 Suite Adaptive Rulesets provide code-independent policy support for registration and authentication. The policies can use multiple inputs including strong signals generated by the S3 Suite App SDKs, contextual information provided by business applications, and risk signals provided by 3<sup>rd</sup> party risk tools.</p> <p>In addition, the S3 Suite Adaptive Rulesets provide 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).</p>
<b>Authentication Protocols and Methods</b>	<p>FIDO UAF, FIDO U2F, FIDO2, WebAuthn - including synced passkeys, device-bound passkeys, attestation and FIDO Metadata. Detection of FIDO security key FIPS certification status and authentication intent as specified by NIST SP 800 63. Enterprise attestation for inventory tracking. Apple App Attest and Google Play Integrity support</p> <p>Nok Nok™ Quick Authentication, Nok Nok™ Intelligent Passwordless Authentication and Nok Nok™ Granular Adaptive Policies</p> <p>Support for Suggestion of authenticator registration, Credential Sharing between Native and Web Applications, End-User preferred custom authenticator names</p> <p>Out-of-Band: QR-codes &amp; push notifications. App-less Out-of-Band Authentication</p> <p>Support for PSD2-SCA, W3C Secure Payment Confirmation (SPC), 3DS2-delegated authentication and dynamic linking (non-repudiation)</p> <p>Email-OTP, SMS-OTP and Photo ID + Live Picture (Selfie) through third-party services</p> <p>OpenID Connect (OIDC) and Security Assertion Markup Language (SAML) support through 3<sup>rd</sup> party IAM systems</p>
<b>Device &amp; Risk Signals</b>	<p>Known device, device health, device model, device type, device manufacturer, device OS version, App SDK version, IP address, location, velocity, Wi-Fi network, device "on-call", and friendly fraud. Supports context data for easy integration with third party provided risk engines and behavioral biometrics systems.</p>
<b>Administration Console</b>	<p>Web-based UI for managing the Authentication Server. Allows administrators to configure policies, change properties, export and import configurations, and review server analytics details.</p>
<b>Granular Administrator Permissions</b>	<p>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.</p>
<b>Multi-Tenancy Support</b>	<p>Serve multiple segregated user groups from a single authentication suite to improve operational efficiency</p>
<b>Reporting and Analytics</b>	<p>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.</p>
<b>Integration</b>	<p>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").</p> <p>Integration with Keycloak, ForgeRock® Identity Platform, Microsoft® Azure B2C and PingFederate®. Customizable sign-in app and credential management page as federated app.</p>
<b>Authentication Server Supported Platforms</b>	<p><b>Cloud platforms:</b> AWS, Microsoft Azure, Google Cloud Platform</p> <p><b>Operating Systems:</b> Rocky Linux 9, RHEL 8, RHEL 9,</p> <p><b>Java:</b> Adoptium and Red Hat OpenJDK 17 and 21, Oracle JDK 17, Oracle JDK 21. Bouncy Castle Java FIPS 1.0.2.x</p> <p><b>Application Server:</b> Apache Tomcat 10.1</p> <p><b>Databases:</b> Oracle 19c and 23c; MySQL 8.0 and 8.4; PostgreSQL 14, 15, and 16; AWS Aurora</p> <p><b>DevOps:</b> Cloud deployment toolkit with Docker and Kubernetes support. Base image: Red Hat UBI9 by default. Custom base images with one of the supported operating systems can be used.</p> <p><b>IoT Support:</b> Through Nok Nok's IoT SDK (licensed separately); IoT SDK authenticates users to IoT devices</p> <p><b>Also available as FedRAMP High and DoD IL5 service through UberEther</b> (<a href="https://uberether.com/">https://uberether.com/</a>)</p>
<b>App SDK Supported Platforms</b>	<p><b>Platforms:</b> Android 5.0+, Wear OS 1.0+, iOS 8+, watchOS 4.2+, JavaScript with WebAuthn API</p> <p><b>Programming environments:</b> Objective-C, C++, Swift, Cordova, Java, JavaScript, ReactJS</p> <p><b>App types:</b> 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</p> <p><b>Widgets:</b> Sign-in, Transactions, Sign-up, Credentials – with fully customizable UI.</p> <p><b>Secure Hardware:</b> Secure Elements, Trusted Execution Environments (TEE), Secure Enclave</p> <p><b>Authenticators:</b> 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</p>



#### 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.