S3 Authentication Suite v9.2 for US Government and Suppliers

DATASHEET

US Government agencies are mandated by Executive Order EO 14208 and Memorandum M-22-09 to implement phishing-resistant authentication for their employees and to offer phishing-resistant authentication to citizens. The Cybersecurity & Infrastructure Security Agency (CISA) **"strongly urges system administrators and other high-value targets to implement or plan their migration to phishing-resistant MFA"** and identifies FIDO/WebAuthn as the **"only widely available phishing-resistant authentication"** solution. FIDO credentials and passkeys can be created and used by users that are not PIV eligible and they can also serve as derived PIV credentials according to FIPS 201-3, to simplify the use of mobile devices.

The Nok Nok™ S3 Authentication Suite (S3 Suite) provides phishing-resistant authentication that can easily be used on mobile devices and PCs without requiring additional middleware or hardware. This scalable approach works well for both workforce authentication and citizen authentication requirements.

The S3 Authentication Suite's rules engine makes it easy to achieve defined authentication assurance levels. M-22-09 also encourages agencies **"to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems."** Nok Nok's Intelligent Passwordless Authentication can restrict authentication to FIPS certified FIDO security keys to achieve NIST SP 800-63 AAL3 or verify appropriate user authentication intent to achieve AAL2 using FIDO passkeys.

The S3 Suite can integrate easily with existing Identity Access Management (IAM) systems such as Keycloak, PingFederate and ForgeRock through optimized adapters. 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
Adaptive Rulesets	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 3rd party risk tools. 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).
Authentication Protocols and Methods	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. Nok Nok™ Quick Authentication, Nok Nok™ Intelligent Passwordless Authentication and Nok Nok™ Granular Adaptive Policies. 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 Email-OTP, SMS-OTP and Photo ID + Live Picture (Selfie) through third-party services
Device & Risk Signals	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”, friendly fraud. 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, export and import configurations, 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 from a single Authentication Suite to improve operational efficiency.
Reporting and Analytics	View, generate, and download statistical data and authentication reports. Provide user-based 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”). Adapters connect to Keycloak, ForgeRock® Identity Platform and PingFederate®. Customizable sign-in app and credential management page as federated app.
Authentication Server Supported Platforms	**Cloud platforms:** AWS, Microsoft Azure, Google Cloud Platform **Operating Systems**: Rocky Linux 9, RHEL 8, RHEL 9, **Java**: Adoptium and Red Hat OpenJDK 17 and 21, Oracle JDK 17, Oracle JDK 21. Bouncy Castle Java FIPS 1.0.2.x. **Application Server**: Apache Tomcat 10.1 **Databases**: Oracle 19c and 23c; MySQL 8.0 and 8.4; PostgreSQL 14, 15, and 16; AWS Aurora **DevOps**: 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. **IoT Support:** Through Nok Nok’s IoT SDK (licensed separately); IoT SDK authenticates users to IoT devices **Also available as FedRAMP High and DoD IL5 service through UberEther** (https://uberether.com/)
App SDK Supported Platforms	**Platforms**: Android 5.0+, Wear OS 1.0+, iOS 8+, watchOS 4.2+, JavaScript with WebAuthn API **Programming environments**: Objective-C, C++, Swift, Cordova, Java, JavaScript, 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, Transactions, Sign-up, Credentials – with fully customizable UI. **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

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.

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