S3 Authentication Suite

At-A-Glance

The Nok Nok™ S3 Authentication Suite integrates into existing security environments to deliver a cost-effective, future-proof and standards-based authentication solution. The Nok Nok™ S3 Suite delivers risk-based, strong authentication for mobile and web-based applications. It includes a Universal Server that supports all FIDO protocols and a variety of value-added features required for a large scale production grade deployment. With the newly introduced ID Proofing and Account Recovery features, the Nok Nok S3 Suite supports the entire authentication lifecycle journey for the end user. The Nok Nok S3 Suite provides support for user authentication lifecycle including identity proofing, registration, authentication, suspend/resume, account recovery and deregistration.

Business Challenges

User Experience

As users interact with a variety of applications on their devices, a seamless and consistent user authentication experience across mobile and PC devices becomes very important. End users want a low friction authentication experience with available biometric options. User testing at Amazon has illustrated that only 40% of customers who forget their passwords attempt to recover them, resulting in a potentially significant loss of revenue.

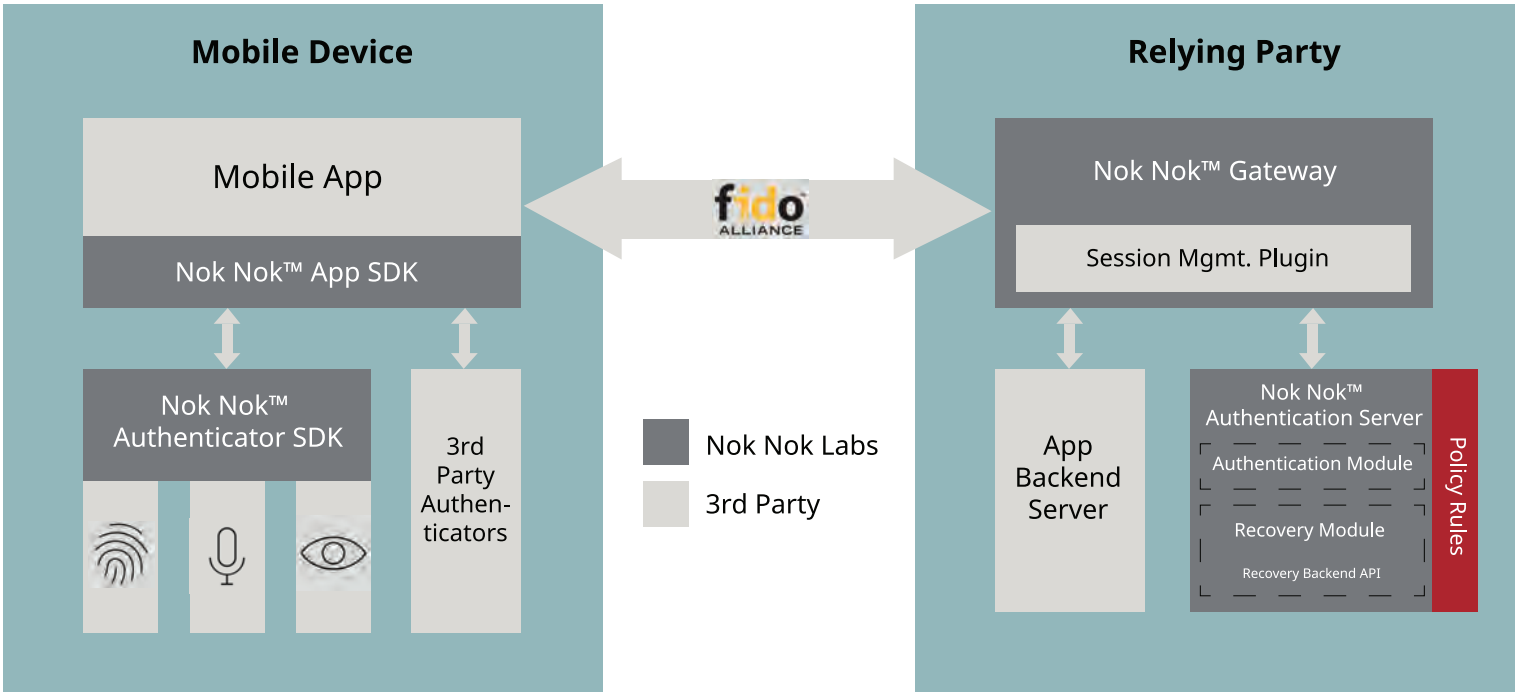
Strong Security

Authentication is the first line of defense for any secured application. However, authentication which relies only on a username+password is failing today's organizations security and usability requirements. According to the Verizon Data Breach Report, more than 80% of attacks are attributed to password vulnerabilities. One Time Passcode (OTP) schemes (e.g., SMS-OTP) don't provide strong security as they continue to be vulnerable to real-time phishing attacks. Trust in SMS-OTP security is decreasing (e.g., see NIST SP 800-63 rating as restricted authenticator with the announcement that it might be deprecated soon). Knowledge-based Authentication (KBA) is not secure either — as it has become easy to obtain the information through social networks or by purchasing it.

Increased Costs

There is a proliferation of devices, platforms, and applications in today's connected world. This means that you need to provide strong authentication for each application on every device and platform type, which can lead to a great deal of complexity and increased costs. The use of costly authentication methods, such as proprietary tokens, knowledge-based authentication and password-based authentication that requires customer support for password resets, only adds to the cost of providing strong authentication. Even today's most successful organizations struggle to balance strong password security protocols with frictionless user experience and revenue-enhancing business practices.

Solution Overview



The Nok Nok S3 Authentication Suite is the first universal server certified for all FIDO protocols (UAF, U2F and FIDO2/WebAuthentication) and is widely deployed globally. Built for simplicity, strength, and scalability, the Nok Nok S3 Suite integrates with a wide range of mobile devices and FIDO Certified biometric authenticators including fingerprint, voice and face biometrics, as well as non-biometric authenticators, such as PIN. It supports a variety of use cases across Business to Consumer (B2C) and enterprise scenarios. The B2C use cases include strong authentication for Mobile and Web application users, ATMs, kiosks and IoT use cases such as connected cars and connected homes. The supported enterprise use cases include strong 1st factor and 2nd factor authentication for internal employees.

The Nok Nok S3 Authentication Suite simplifies strong authentication by leveraging existing security capabilities available on most mobile devices and PCs. The solution enables any application to employ these capabilities by plugging them into an end-to-end framework based on the FIDO protocols: UAF, U2F and FIDO2/WebAuthentication. The Nok Nok S3 Authentication Suite allows organizations to consolidate multiple authentication stacks into one simple unified solution to reduce the cost and complexity.

Core components include:

Nok Nok Authentication Server

The Nok Nok Authentication Server enables multi-factor authentication for organizations with internet-scale mobile and web applications. It allows businesses to use standards-based authentication to rapidly support new devices, improve user engagement, reduce fraud, and minimize costly password resets.

The Nok Nok Authentication Server implements a Universal Server supporting all FIDO protocols, including the latest FIDO2/Web Authentication standards, and supports all mobile, web and emerging IoT use cases through a customer's entire digital journey. The W3C Web Authentication standard is supported by leading browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, etc., making it possible to deploy FIDO2 for web applications at scale. In addition to the on-premise deployment model, the Nok Nok Authentication Server is also available in Software-as-a-Service (SaaS) model.

Federation Connectors

The Nok Nok S3 Suite features out-of-the-box integration with popular federation systems such as ForgeRock OpenAM, and Ping Identity PingFederate. It provides strong authentication for SAML and OpenID Connect-based infrastructure for more rapid deployment. Alternatively, the Nok Nok Authentication Server can be directly integrated with applications via a simple REST API.

Nok Nok Gateway

The Nok Nok Gateway further simplifies the integration of the S3 Suite. The Gateway acts as a proxy and therefore, allows the Nok Nok Authentication Server to be deployed behind firewalls in higher security network zones, and does not expose it to the Internet. By using the simplified integration approach, the back-end integration is also easy and limited to just developing a Gateway session plug-in.

Nok Nok App SDK

The Nok Nok App SDK allows enterprises to rapidly support heterogeneous device populations that include Android and iOS mobile apps and web applications along with diverse authenticators such as Apple Touch ID and Face ID, as it eliminates the need for users to carry separate tokens for authentication. Organizations incorporate the App SDK into their mobile app or web application to deliver on-device authentication, or to enable their mobile app or web application to provide out-of-band authentication for access initiated from another device. The App SDK takes advantage of available secure hardware, such as Trusted Execution Environments (TEE), Secure Elements (SE) and Trusted Platform Modules (TPM) to protect critical components of authentication on the device.

Key Capabilities

Identity Proofing and Account Recovery

The Nok Nok S3 Suite provides a flexible policy based platform for identity proofing and account recovery. Identity proofing is supported via variety of methods including email ID, phone number and scan of government issued Photo ID and a live picture. Account recovery can be done via the above methods as well. Using the account recovery policies, these recovery methods can be enforced in any combinations using “AND” and “OR” operations to achieve desired security. The account recovery platform is scalable and any additional recovery method can be added to it easily.

Consistent Omni-Channel Authentication

By deploying the Nok Nok S3 Suite with support for UAF, U2F and FIDO2 protocols, you get support for strong and authentication on all platforms including mobile, web, ATMs, call centers and more. With the support for all FIDO protocols, the customers can use the same authentication modalities (e.g. Fingerprint, Face Recognition etc.) in the native App and in the Browser. This results in a consistent user experience across all platforms.

Multi-Modality

The Nok Nok S3 Suite supports authentication on mobile and PC devices using the device’s default modality. The Nok Nok S3 Suite supports any existing and future authenticator modalities including biometric modalities like face and voice as well as PIN, user presence and silent authentication. This reduces the overall reliance on passwords.

Risk Signals

A policy-driven risk and intelligence engine module augments FIDO-based authentication with risk signals based on user and device geolocation, travel speed, device ID and other factors to further evaluate the risk posed by each attempted authentication. By first taking into account the established profile of the user and then monitoring for anomalies, organizations can either deny access outright for deviations from expected behavior, or calculate a risk score that will determine whether or not to approve access.

Reporting and Analytics

The Nok Nok S3 Suite provides rich analytics and historical reporting, which can be used to support analysis of user behavior for system optimization, fraud reduction, improved convenience, acceptance, cost reduction, etc. It also support tamper-evident audit logs for regulatory compliance.

Key Benefits

Reduced Attack Surface

The Nok Nok S3 Suite eliminates the need for shared secrets such as static and one time passwords (OTPs). Superior to traditional passwords, OTPs mitigate some risks. But because modern malware can circumvent OTP security regardless of the use of hardware, software or SMS OTP tokens, OTPs offer minimal additional protection against an advanced adversary. By leveraging secure hardware, the Nok Nok S3 Suite removes the need to transmit or store sensitive passwords or biometric data in the server. This results in no additional password or OTP seed databases to secure, no easily guessed or reused passwords, and added protection against phishing and malware attacks.

Assured Privacy

The Nok Nok App SDK takes advantage of secure hardware to give the user security and control over their data. Because all user biometric data remains securely on each personal device, privacy is maintained. And because no identifiable information needs to be held by the organization, the burden of securing it is eliminated.

Minimized Authentication Costs

By leveraging the standards-based FIDO protocol and the Nok Nok App SDK support for over a billion Android and Apple devices, the Nok Nok S3 Suite can address all the devices your users currently employ. It can expand to address new, more advanced biometric capabilities available on current and future devices. This minimizes the cost of developing support for new authenticators and further reduces operational costs as the industry standard approach removes the need for authentication silos and supports the bring-your-own-authenticator (BYOA) concept.

Increased Revenue

Consumers that can sign in through familiar, user-friendly biometric authentication methods on their own devices will be more satisfied, and less likely to abandon their shopping carts or move to a different application. Password avoidance improves the experience and promotes user engagement. Revenue increases as consumers adopt new apps and use them more frequently to complete more transactions.

Regulatory Compliance

Nok Nok Authentication Server supports audit logs which help you meet various industry regulations requirements such as GDPR, PSD2, SOX and HIPAA.

Find out more

For more information on Nok Nok and S3 Authentication Suite, please visit www.noknok.com. 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/trynow .

ABOUT NOK NOK LABS

Nok Nok empowers global organizations to improve the user experience to access digital services, while meeting the most advanced privacy and regulatory requirements. Nok Nok Labs and its industry leading customers and partners include Fujitsu Limited, Ericsson, Hitachi, Lenovo, NTT DATA, NTT DOCOMO, OneSpan and Samsung. For more information, visit www.noknok.com.

November 2018