In an era of increasing, high-profile security breaches, protecting your company and your customers is more critical than ever. But at the same time, simplifying customer access to your apps would help to drive additional revenue, increase engagement and ensure continued loyalty.

The truth is, you don’t have to choose between security and usability. With today’s new biometric technologies, you can have both.

Nok Nok Labs S3 Authentication Suite delivers organizations the infrastructure necessary for risk-based, strong authentication supporting the FIDO® specifications for mobile and web-based applications. The NNL™ S3 Suite allows businesses deploying consumer-facing apps to leverage biometrics for both enhanced security and a superior user experience, all while substantially lowering the costs associated with authentication.

The Nok Nok Labs S3 Authentication Suite allows organizations to:

- Improve customer satisfaction rates, increase user engagement and drive revenue through an unparalleled, biometrics-enabled user experience
- Enhance security by eliminating the threat of password theft commonly associated with large scale security breaches
- Reduce authentication costs with minimal development requirements and fewer password reset or assistance calls
- Enable simple, secure access to apps operating on all major mobile platforms
- Leverage a user’s mobile device to enhance security while accessing apps from another device
- Easily future-proof for new biometric technologies and device capabilities
- Preserve user privacy through local storage of personal data
Passwords are failing today’s organizations. 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. At the same time, nearly two-thirds of all confirmed data breaches are in some way password related.

Even today’s most successful organizations are struggling to balance strong password security protocols with revenue-enhancing business practices.

To successfully address these issues, organizations require a new approach to authentication that combines security with simplicity – and biometrics has emerged as the solution. By ensuring the protection of user identities while also eliminating the friction that prevents customers from completing transactions, biometrics delivers state-of-the-art security that actually helps business to grow.

**Client-side biometrics**

After evaluating both client-side and server-side biometrics options, the majority of today’s enterprises are selecting client-side biometrics, because it combines a better user experience with a higher level of security when implemented as advocated by the FIDO Alliance and the FIDO specifications. Unlike server-side biometrics, client-side solutions allow for multifactor authentication and virtually eliminate the potential for losing customer data when a server is hacked.

A client-side FIDO Certified biometric approach means that all biometric information is securely maintained on the user’s personal device and is never sent to a server. This avoids reliance on the security of a deploying organization and mitigates the possibility of a scalable attack. Because maintaining user privacy is paramount, this client-side approach to storing biometric is ideal.

After several years of success in the public sector, biometrics has matured and is now entering the market en masse. This proliferation enables software solutions from Nok Nok Labs to offer an advanced infrastructure capable of leveraging client-side biometrics technologies for multi-factor authentication for millions of users across a multitude of devices. Companies are now implementing these technologies to enhance mobile app security and drive additional revenue through improved user convenience.
The Nok Nok Labs S3 Authentication Suite is the first and only full-featured, FIDO-Certified authentication platform solution in the market. Built for simplicity, strength and scalability, the 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.

The NNL S3 Authentication Suite simplifies strong authentication by leveraging the existing security capabilities available on most mobile devices. The solution enables any application to employ these capabilities by plugging them into an end-to-end framework based on the FIDO Universal Authentication Framework (UAF) Protocol. Through the FIDO UAF, users can quickly and securely authenticate through a variety of methods available today, as well as support emerging technologies – all without the need to store and manage user passwords. The newly added FIDO U2F protocol support allows online services to augment the security of their existing password infrastructure by adding a strong second factor.

The NNL S3 Authentication Suite allows organizations to consolidate multiple authentication stacks into one simple, unified solution. Its core components include:

**Nok Nok Authentication Server**

The Nok Nok Authentication Server enables multifactor authentication for organizations with Internet-scale mobile apps. It allows businesses to use standards-based authentication to rapidly support new devices, improve user engagement, reduce fraud and minimize costly password resets. The Authentication Server features out-of-the-box integration with popular federation systems (such as ForgeRock OpenAM, Ping Identity PingFederate and others) and provides strong authentication for SAML and OpenID-based infrastructure for more rapid deployment. Alternatively, the Nok Nok Authentication Server can be directly integrated with applications via a simple REST API.

The Authentication Server offers a policy-driven risk and intelligence engine module that sets the solution apart from other biometrics-based authentication systems. This powerful platform 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. The risk engine is essential in minimizing online fraud.

**Nok Nok App SDK**

The NNL 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. The App SDK allows enterprises to rapidly support heterogeneous device populations that include Android and iOS along with diverse authenticators such as Apple Touch ID as it eliminates the need for users to carry separate tokens for authentication. Organizations incorporate the App SDK into their mobile app to deliver on-device authentication or to enable their mobile app to provide out of band authentication for access initiated from another device.
**Reduced attack surface**
The S3 Suite eliminates the need for shared secrets such as static and one time passwords (OTPs). Superior to traditional passwords, OTPs mitigate some risk. But because modern malware can circumvent OTP security regardless of the use of hardware OTP tokens, software OTP tokens, or SMS tokens, OTPs offer minimal additional protection against an advanced adversary. By leveraging secure hardware, the S3 Suite removes the need to transmit or store sensitive passwords or biometric data. This results in no more password or OTP seed databases to secure, no more easily guessed or reused passwords, and added protection against phishing and malware attacks.

**Increased revenue**
Consumers that can log 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.

**Wide use case coverage with FIDO-based out-of-band authentication**
Users leverage their existing mobile devices to authenticate and approve transactions initiated from another device via another channel, such as a web-based application accessed with a laptop. The user may choose to authenticate through the mobile device, inside the app or via a mobile browser. New devices may also be bootstrapped, allowing the user to move from one device to another with ease – and without relying on passwords or other account recovery mechanisms to enable a new device.

**Assured privacy**
The Nok Nok Labs 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.