TECHNICAL WHITE PAPER

ENABLING BIOMETRICS FOR MOBILE APPLICATION AUTHENTICATION

Comparing Nok Nok S3 Authentication Suite and Native API Approaches

Nok Nok
LABS

EXECUTIVE SUMMARY

In an increasingly mobile world, relying on username and password-based authentication is simply proving to be untenable. Using biometrics for consumer-facing mobile application authentication is an emerging enterprise imperative that delivers both ease of use and improved security. There are several different ways to utilize biometrics for mobile application authentication. One approach is to integrate biometrics such as fingerprint authentication using native, or platform-specific, application programming interfaces (APIs) from mobile platform and device vendors. This paper offers an in-depth look at the required resources and risks associated with the native API approach and it explains how Nok Nok Labs enables organizations to embrace biometrics while avoiding native API drawbacks.

THE BIOMETRIC IMPERATIVE FOR MOBILE APPLICATION AUTHENTICATION

Keeping Up With An Evolving FIDO Specification

Many online and mobile applications handle items of value—financial transactions, personally identifiable information, confidential information, and more. Guarding access to these applications via strong authentication is essential, but current password-based approaches deliver a poor user experience, offer inadequate security, and introduce increasing costs and risks. Consequently, by relying on authentication via usernames and passwords, enterprise risk is increased and organizations' revenues and profits suffer.

Biometric authentication is emerging as a strategic mandate for enterprises deploying consumer-facing applications. Biometrics can help organizations overcome the limitations of usernames and passwords and improve user experience and security. Recent advances in the mobile technology landscape, such as the widespread production of smartphones with fingerprint sensors, make biometric authentication an appealing alternative to usernames and passwords.

Enterprises deploying consumer-facing mobile applications have several options to consider in implementing biometric mobile authentication. Organizations can use libraries from third parties and APIs from device manufacturers and operating system (OS) vendors. For example, to exploit fingerprint recognition capabilities on mobile devices, organizations can leverage native APIs for the Apple iOS or Android platform.

While native APIs may seem to provide a quick path to establishing the desired functionality, such approaches require significant investment and can introduce significant risks (see the below sidebar). The following sections examine the required resources and risks in detail.

Risks Associated with Native APIs for Mobile Authentication

- **Security risk.** Building an authentication environment that delivers end-to-end security requires deep expertise and focus—attributes that may require internal investment to establish and maintain. In short, authentication takes significant expertise to do right—and if its not done right, the consequences can be disastrous.
- **Financial risk.** The larger the up-front investment associated with an authentication implementation, the longer it may take to recoup costs. How long will it take to recoup the significant costs of building a native-API based authentication solution? In addition, there are a number of scenarios that can result in this investment never realizing the expected ROI. For example, what happens if the expected business benefits of fingerprint authentication do not materialize? What if the business discovers that the initial approach fails to address the required use case? What if customer preferences change? If a new security threat arises that leaves the implementation exposed? Will a native implementation deliver flexibility to address future methods of biometric authentication?
- **Development risk.** An internally sourced implementation requires proprietary code and integration, which means that the business is dependent on internal staff members that know the code and how to maintain and enhance it. An authentication platform may have a shelf life of a decade or longer. However, the average tenure for employees is 3.68 years.[1] What happens when key employees leave? How will development teams ensure internal staff are always available to handle ongoing updates, and how will they cost-effectively ramp up to accommodate increasing and evolving requirements?
- **Competitive risk.** An in-house native API implementation can take considerable time to deploy to market. What happens if an application provider's competitors roll out biometric approaches that are more secure and deliver a better user experience, well before the organization can get its own solutions deployed?
- **Opportunity cost.** Executives have to decide how to allocate their organization's finite resources. If an organization invests significant time and capital in developing a native API authentication implementation, that means those resources can't be applied to other more strategic projects. What happens if pursuing this implementation precludes the business from capitalizing on lucrative opportunities to support new customers or generate new revenue streams?

[1] Payscale, "The Most and Least Loyal Employees," URL: http://www.payscale.com/data-packages/employee-loyalty

KEY FACTORS TO CONSIDER BEFORE IMPLEMENTING BIOMETRIC AUTHENTICATION USING NATIVE APIS

Supporting the Large-scale Effort Required to Build a Strong, Complete Security Solution

When organizations take on the implementation of biometric authentication via native APIs, they assume a major responsibility. As the onslaught of headline-grabbing data breaches continues to show, vulnerabilities associated with user credentials continue to be sought, targeted, and exploited—often leading to brand damage, financial penalties, staff turnover, and other disastrous consequences for victimized businesses.

Security is only as good as the weakest link in the chain. While native APIs provide a toolkit for development, it is ultimately the application developer's responsibility to build a complete solution that provides comprehensive security. Application architects need to consider the end-to-end authentication process, from the end-user device through to the backend server and infrastructure, and all transmissions and processes in between.

Authentication is comprised of two key aspects: authenticating the user locally on the device, and authenticating the device to the authentication server at the backend. While native APIs support the process of authentication on the device, they do not deliver functionality for authenticating to a remote server. Establishing a highly secure system that supports this remote authentication represents a significant undertaking. The application development team must take responsibility to architect all the security mechanisms, implement the required infrastructure, provide a test environment for heterogeneous devices, do penetration testing, and so on.

> **"As a result of having fallen into app development as a business necessity, organizations are typically lacking in basic app development life cycle skills such as user experience (UX) design, quality assurance, mobile-specific back-end data integration and mobile-oriented security needs."**
>
> **Gartner, "How to Build a Successful Mobile App Development Team", Adrian Leow, Nick Jones, Richard Marshall, 19 October 2015**

These activities do not just entail significant effort; they also demand high levels of expertise. When employing a native API-based approach, organizations will need security-savvy engineers to orchestrate a complex sequence of processes, which can be difficult to implement. Building authentication solutions is typically not a core competency, nor a primary area of focus, for internal development teams delivering consumer-facing applications. Consequently, many internal native API implementations are prone to risks:

- **Insecure transmission.** By employing native APIs, an organization can enable the user to authenticate with a fingerprint. However, in many cases, the development team will set up the remaining backend infrastructure to rely on passwords or other user credentials, such as tokens stored on both the server and client device. After the initial authentication on the device, credentials sent over the wire to the backend authentication process may be exposed to man-in-the-middle and phishing attacks.
- **Insecure handling of credentials.** Another common concern in native API deployments is the insecure handling of credentials on the mobile device. For example, rather than using secure hardware on the device, some development teams will only use application logic to safeguard credentials. As a result, if the application is compromised, user credentials may be exposed as well.[2]
- **Compromised devices.** Particularly for high-value transactions, it is important that the integrity of the device can be validated through attestation. Specifically, when credentials are passed to the remote authentication server, organizations need to distinguish between a legitimate user and someone attempting to exploit the API with compromised credentials. Increasingly, mobile devices are being developed that support this attestation process and application providers should leverage these capabilities whenever possible.

[2] The Register, "Banks defend integrity of passcode-less TouchID login", John Leyden, March 19, 2015, URL: http://www.theregister.co.uk/2015/03/19/rbs_defends_banking_security_touchid_login_iphone_apple/

Supporting the Myriad Combinations of User Devices, Heterogeneous Platforms, and Authenticators—Now and as Requirements Change

In addition to the security requirements above, supporting an organization's biometric authentication strategy via a native API approach will require multiple development projects to cover major platforms, various versions of those platforms, and potentially several authenticators on those platforms. A distinct development, testing, and patching effort may be required for each authenticator on each device model or OS. The costs associated with these efforts can grow exponentially as biometric methods become more popular and new approaches and platforms are brought to market.

Support for Multiple Device OSs and Versions

In today's heterogeneous world, supporting multiple device platforms, versions, and types is a critical success factor for any consumer-facing application. However, each API from a mobile OS vendor only supports the native OS. Therefore, in order to establish the device coverage required, application providers may need to build distinct authentication solutions for each device's native API.

Each native API implementation will have to be independently developed, tested, published, and maintained. As result, this approach will require a large-scale effort, one that is replicated for each platform to be supported. Further, application developers need to accommodate past OS versions to support the installed base of legacy devices, while adding support for new OS releases as they hit the market. This is a particular challenge in supporting the Android market, where a significant number of OS releases are in use at any given time.

Such development efforts are complex. Rather than being centrally architected and managed, an application supporting multiple platforms has different architectures, code streams, and processes. Even with the most talented development teams, such internally developed solutions may be brittle, making it difficult to add new capabilities, without introducing glitches or requiring significant rework and retesting.

Further, this work will never end. Over time, APIs, devices, and use cases change, meaning development teams will have to continue to update code to adapt. Code will need to be redeveloped, retested, and redeployed each time a new version is unveiled and whenever new capabilities are made available via the APIs. Finally, if a new device type is produced, an entirely new development effort will need to be kicked off.

Support for Different Authenticators and Evolving Authentication Approaches

While current native APIs could enable an application provider to support fingerprint-based authentication, the reality is that multiple authentication approaches, devices, and scenarios will need to be supported from day one. Specifically:

- Organizations need to provide a superior authentication experience to all users, not just those with devices that are supported by a specific platform's API.
- Even for those users with devices running on a platform supported by a native API deployment, alternative authentication mechanisms need to be offered. In the case of fingerprint sensors, alternatives are needed in the event a user's fingers are too cold or wet to get a scan, or their phone's sensor is broken.

In the longer term, the variety of biometric approaches seems sure to expand. While fingerprint-based authentication appears to be the front-runner in terms of biometric authentication today, no one knows what the dominant approaches will be in the coming years. Other emerging biometric innovations include iris, facial, gesture, and voice recognition, and these innovations will come from a number of vendors.

Consumer preferences, technological innovation, and security threats continue to accelerate and evolve with increasing speed. Therefore, it is important to quickly adapt to evolving requirements—but native APIs do not facilitate this adaptation. With native APIs, responding to these evolving demands will entail separate, large-scale efforts. Fundamentally, by opting for the use of native API-based development, application providers will take on a labor-intensive, complex series of implementations—and they will limit their ability to leverage future biometric innovations.

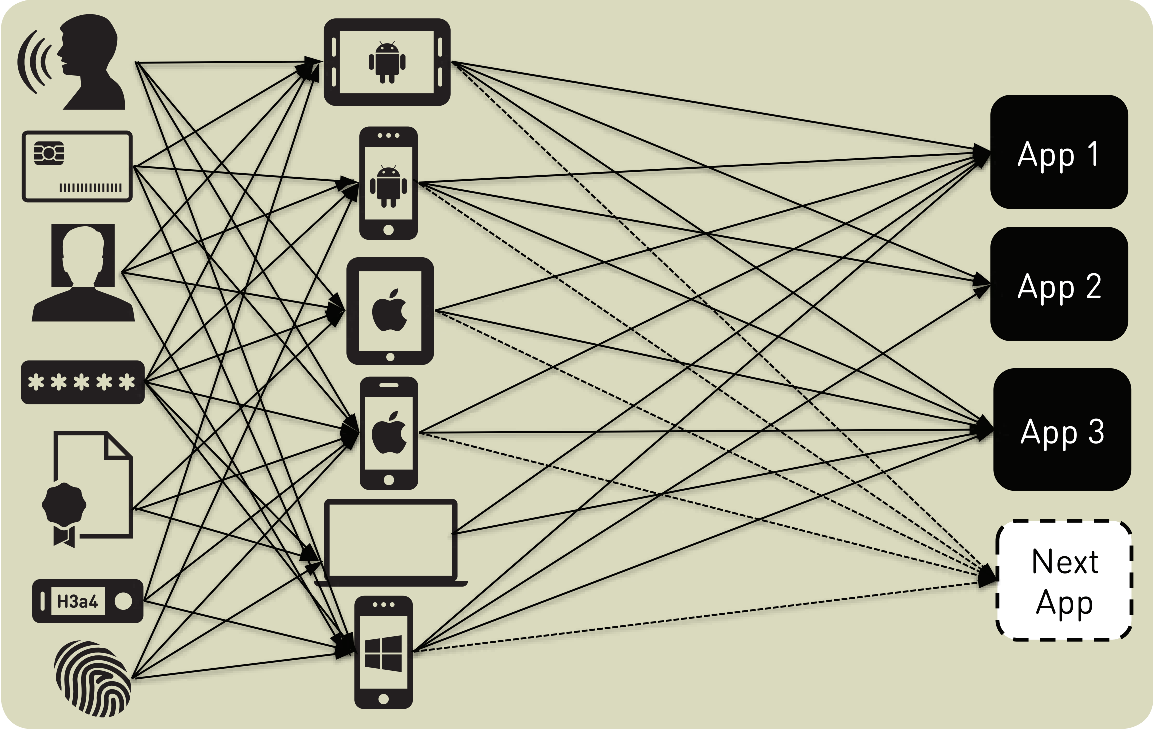

Figure 1: The complexity involved in supporting different authenticators, platforms, and applications

Scaling Deployments to Support Massive User Bases and Transaction Volumes—While Ensuring High Performance and Availability

For an application developer, success will equal growth: growth in the number of users, services, and transactions. When employing native API approaches, a key question is whether an internally developed architecture will support business success or fall apart under stress.

Success requires an application and infrastructure that is massively scalable, as well as high performing and reliable. When it comes to authentication, downtime can result in a direct and immediate hit to revenues. Slow performance can yield a poor user experience that leads to abandoned transactions and lost customers.

Architecting, building, testing, and tuning internal code and infrastructure that can scale to support massive customer bases and transactions will require significant staff time and effort. In seeking to address their organization's scalability and performance demands, development teams need to avoid short cuts that introduce security gaps. For example, a development team could attempt to boost responsiveness by caching passwords, but this approach would introduce significant risks. The business will have to make extensive infrastructure investments to deliver the required performance and resilience. Here again, the stakes are high and the work will never be complete—the environment will need to be monitored, maintained, and optimized for the duration of the deployment.

THERE IS A BETTER WAY: THE NOK NOK S3 AUTHENTICATION SUITE

Today, organizations have a faster, easier, cheaper, and more secure way to adopt biometric authentication—and to manage all their mobile authentication requirements. By leveraging the Nok Nok™ S3 Authentication Suite, organizations can avoid the massive significant costs and risks associated with implementing native APIs. The S3 Authentication Suite is a comprehensive authentication framework that features the following components:

- The Nok Nok™ Authentication Server
- The Nok Nok™ App SDK supporting both Android and iOS devices

The S3 Authentication Suite is built based on the Universal Authentication Framework (UAF) defined by the FIDO® Alliance (see sidebar). By leveraging this standards-based solution, organizations can realize maximum deployment efficiency and long-term flexibility.

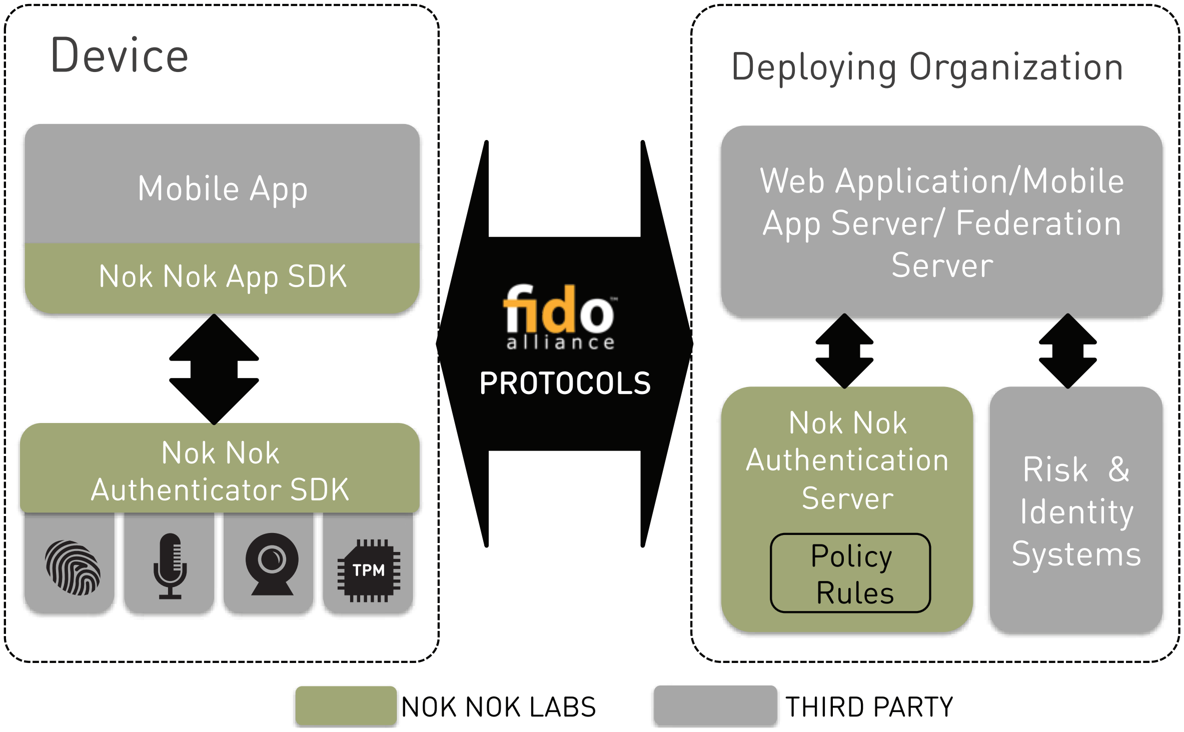

Figure 2: The S3 Authentication Suite architecture

The FIDO Effect: Industry Standard, Industry Proven

The FIDO® ("Fast IDentity Online") Alliance is an industry consortium that was launched in February 2013. Member companies work together to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords. Nok Nok Labs was one of the Alliance's six founding entities. As of 2015, the FIDO Alliance has grown to include over 250 members, including Google, Huawei, Lenovo, LG, Microsoft, PayPal, Samsung, and Visa. The FIDO Alliance has created authentication specifications that enable strong, easy-to-use authentication across a multitude of authenticators, devices, and OSs.

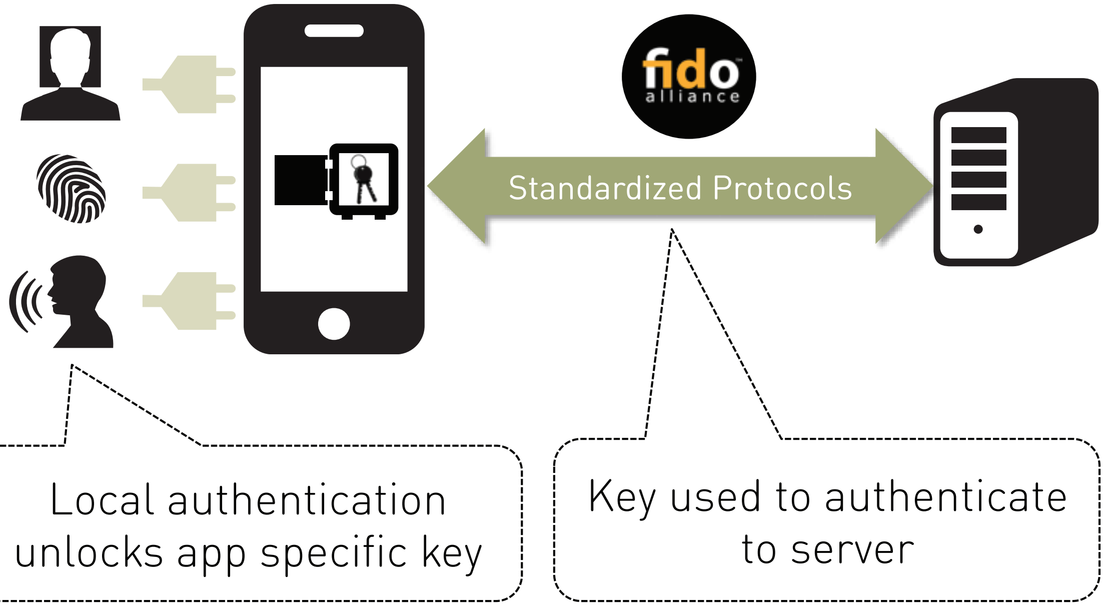
fido alliance
Standardized Protocols
Local authentication unlocks app specific key
Key used to authenticate to server

Figure 3: FIDO protocols enable customers to manage authentication in a more flexible and secure fashion

Delivering Strong, Comprehensive Security

The S3 Authentication Suite represents a complete solution for mobile authentication. The solution supports the entire authentication process from end to end, and it does so in a seamless, highly secure fashion.

To safeguard privacy, biometric matching happens on the device with no biometric data being sent to the server. The S3 Authentication Suite uses private/public cryptographic key pairs, and the server only stores the public keys. Even if these public keys were compromised, they wouldn't enable an attacker to impersonate an authorized user. The private key always stays on the user's device, helping alleviate the risks associated with eavesdropping attacks. Further, the Nok Nok App SDK enables organizations to store keys in hardware, leveraging trusted execution environments and secure elements when available on devices with FIDO UAF-certified authenticators.

When the solution is properly implemented, authentication credentials and confidential keys are never stored in the clear. This helps make the implementation resilient against shoulder surfing, recording keystrokes, and phishing attacks that fool the user into divulging credentials. The solution encrypts communications with TLS, offering strong protections against man-in-the-middle attacks.

The platform enables more robust security by supporting integration in a number of areas:

- **FIDO Certified™ devices.** The S3 Authentication Suite can harness the stronger security capabilities available on FIDO-certified devices, including those from Samsung, Sony, Fujitsu, Sharp, and others. Through this integration, the authentication server can obtain visibility into the device, the characteristics of the device, how keys are protected, how the verification process is handled, and more. Through such metadata, an application provider can more accurately verify that the device and the credentials it provides are authentic.
- **Adaptive risk-based authentication.** With the S3 Authentication Suite, customers can use the FIDO protocol to feed intelligence into their existing risk engines. As a result, they can dynamically assess the level of trust and employ step-up authentication processes when needed.
- **Integration with single sign on (SSO) and identity federation platforms.** While SSO and identity federation can help an organization reduce its reliance on passwords, these approaches can also present concentrated risk: One breach can compromise multiple services. The S3 Authentication Suite offers interoperation with SSO and identity federation solutions, helping secure the "first mile" in the authentication chain.

Comprehensive, Extensible Device and Authenticator Support

Through its flexible architecture and FIDO support, the S3 Authentication Suite provides an extensible solution for managing consumer-facing authentication. With the solution, organizations can quickly address their immediate requirements and they can smoothly migrate to support emerging authenticators as they are delivered to market. Rather than having to embark on a new development project each time a new device or authenticator is released, customers can support new FIDO-enabled devices and authenticators in a plug-and-play fashion, simply by updating policies. The S3 Authentication Suite features:

- **Extensive platform support.** The S3 Authentication Suite leverages Android's latest Marshmallow release, and it also supports legacy Android versions. In addition, it offers support for the iOS platform and Touch ID-enabled devices.
- **Broad authenticator coverage.** By abstracting the details of local authentication from the server, the solution enables any authentication method to be used. With the solution, customers can support not only fingerprint sensors but also iris, facial, voice, and other authenticator types.
- **Out-of-band (OOB) authentication support.** Through its OOB authentication capabilities, the S3 Authentication Suite enables organizations to support non-FIDO and even non-mobile devices. As a result, an application provider could have consumers use a mobile device to authenticate to a separate target system, such as a laptop, smart TV, ATM, or kiosk.

Enterprise-grade Performance, Availability, Scalability

The S3 Authentication Suite represents a complete, pre-packaged solution. By leveraging a commercially supported offering that is standards-based and integrated, organizations can realize high performance and availability—and eliminate the need to build and optimize their own infrastructure and code. The solution has been proven to deliver the performance, scalability, and availability that the largest application providers require. The S3 Authentication Suite has been commercially deployed at scale in production environments at a range of organizations, including Alipay, NTT DOCOMO, and PayPal.

CONCLUSION

There is little debate around the need to leverage biometric authentication to overcome the limitations associated with password-based approaches. The key question for a developer considering adopting biometrics is this: How does an organization address its biometric authentication requirements quickly and cost effectively, but without compromising security? Employing native APIs falls significantly short of addressing these key objectives. With the S3 Authentication Suite, organizations can leverage a commercially supported solution that eliminates the resource costs and risks associated with native API-based approaches. The S3 Authentication Suite enables organizations to quickly address their immediate requirements, and enjoy maximum flexibility to adapt as security, business, and technological needs evolve in the future.

ABOUT NOK NOK LABS

Backed by a team of security industry veterans from PGP, Netscape, PayPal, and Phoenix, Nok Nok Labs has deep experience in building internet- scale security protocols and products. Our ambition is to fundamentally transform authentication, by unifying authentication into one standard protocol, giving business the power to make the utmost of the cloud, data, mobile, and business online.

Nok Nok Labs
2100 Geng Road, Suite 105
Palo Alto, CA 94303

www.noknok.com

TO LEARN MORE ABOUT NOK NOK LABS, VISIT NOKNOK.COM OR CONTACT US AT INFO@NOKNOK.COM

Nok Nok
LABS