WHITE PAPER

STRONG AUTHENTICATION: IT IS TIME TO ACT.

Any device.
Any application.
Any authenticator.

Nok Nok
LABS

TABLE OF CONTENTS

In the Interests of an Organization........3
If Implemented Correctly... 4
The Expert in Implementation........5
A Time of Convergence 6

Nok Nok
LABS

Nok Nok Labs has released the S3 Authentication Suite, a product certified by the FIDO Alliance that empowers an organization to have scalable, strong and simple authentication. Access has become the cornerstone of an organizations ability to transact business and all signals are pointing to one conclusion: It is time to deploy Strong Authentication.

IN THE INTERESTS OF AN ORGANIZATION

The modern world is one where every campaign has online and mobile components that are core pillars of its strategy. The realities of the online landscape require multiple parts of an organization to come together over a single value proposition: **Friction gets in the way of providing goods and services to users.** Some parts of an organization advocate that the benefits of some actions outweigh the friction that they introduce. For example, requiring capital letters, numbers, special symbols in passwords make those passwords more difficult to crack using a dictionary-based hack – but they introduce friction in creating, submitting and remembering the details of the new, "stronger" password. The argument that the password is now "more secure" and, therefore, decreases fraud swayed the minds of the stakeholders who initially made the decision. After all, the secret that is shared between the organization and the individual is now so unique as to make it virtually un-guessable.

However, with the rise of these more complicated passwords, we have seen a matching increase in the phenomena of cart abandonment, a decrease in return customers, an increase in calls to the customer support line to reset the password, and a significant decrease in customer satisfaction. Couple this need for a stronger shared-secret to the new methods by which we are submitting our passwords and you can see yet another weakness of our traditional models. Typing in our password on a tiny touch screen with equally small keys and an over-eager auto-correct and we are more likely to throw our smartphone into the wall than we are to gain access to our account on the first try.

> Organizations are losing revenue, losing customers, increasing costs and increasing the cost of acquiring new customers – all due to the problem of passwords.

The questions then persist: how can an organization establish the identity of an individual to ensure that products are purchased, services delivered, accounts are transferred? How can an organization authenticate its users without the use of a shared-secret like the password?

Technology, it seems, has finally caught up to where our ancestors were generations ago. When walking into a general store, identity was confirmed through facial recognition – something you were. The ability to pay for a thing rested in your ability to produce cash - something you had. Having your dry goods delivered to you required you to produce your address – something you knew. Multifactor authentication (a requirement of having two of the previous three categories) is strong authentication and strong authentication is available today.

A strong authentication solution will create an experience for the user that is virtually frictionless. If implemented correctly, strong authentication will provide the signals necessary to generate high confidence in the identity of the user, thereby decreasing the threat of fraud. Strong authentication does not rely on shared-secrets – eliminating the need for a massive database to sit as a juicy target for some malicious coder to attack. Deployed today – and in the hands of users – are enough of the right kind of devices, the right kinds of sensors and the right kinds of software to enable strong authentication to be deployed across the entirety of an organizations user population. Fundamentally, strong authentication does more than **replace** the username and password paradigm, it moves **beyond it**. With the signals and assurance provided by properly implemented strong authentication, an organization will have the confidence to increase the number of services that they had heretofore provided – opening the door for more revenue, more innovation, more opportunities to grow.

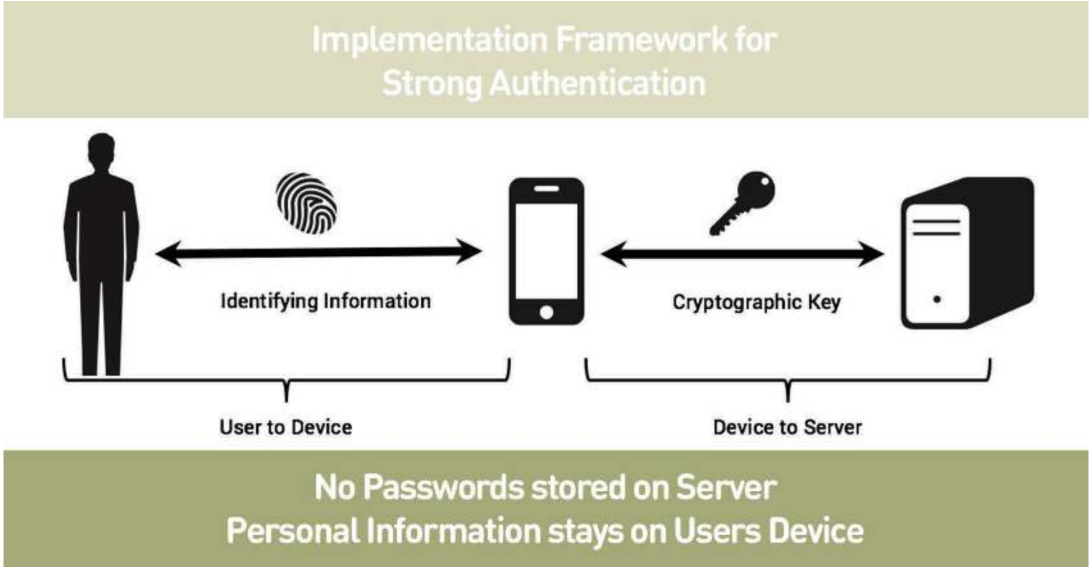
> Strong authentication should be in the interests of every part of an organization. Why? Because the value proposition of "Friction gets in the way of providing goods and services to users" is true – and strong authentication eliminates friction.

If Implemented Correctly...

Several years ago, Nok Nok Labs was a founding member of the Fast IDentity Online Alliance (the FIDO Alliance). The mission of the FIDO Alliance was to publish a set of technical protocols that would enable an organization to replace weak authentication with a framework for strong authentication. The FIDO Alliance, however, was not the first organization to search for a solution to the password problem. There have been attempts to solve authentication by leveraging biometrics, by issuing digital certificates, by delivering physical tokens or issuing one-time-passwords. While each of these solutions have chipped away at the edges of the problem, none were sufficiently comprehensive, some were prohibitively expensive, and others simply made the problem worse.

One of the risks of passwords is the way they are stored; vast databases filled with millions of shared-secrets hidden behind a wall of software security that is only as good as it's last update. The news has been filled with story after story of breaches and fallout. While an organization can have a higher confirmation of a user's identity by using biometric identifiers – if those biometric templates are stored centrally in a server-side database – the cure for passwords will be much worse than the disease. After all, if a password is stolen, it is simple to create a new one. If a fingerprint is stolen, the solution is much less obvious.

How, then, would strong authentication be implemented correctly? Simply put, the FIDO protocol requires that a user authenticates to a device and the device authenticates to a service. At the root of this system is public-private key cryptography. When a user initially registers, the device generates the cryptographic key-pair. The public key is sent to a FIDO server run by an organization. The private key is securely stored on a device. The keys are locked to the user so when a user wishes to access his or her account, he proves to the device who he is. This can take the form of a biometric identifier – like a fingerprint – but it doesn't have to. The organization who is backing the FIDO server has the flexibility to select the modality of their choice for this authentication. Once the user authenticates to the device, the device releases the private key, which is then paired with the public key and access to the account is granted.


Implementation Framework for
Strong Authentication
Identifying Information
Cryptographic Key
User to Device
Device to Server
No Passwords stored on Server
Personal Information stays on Users Device

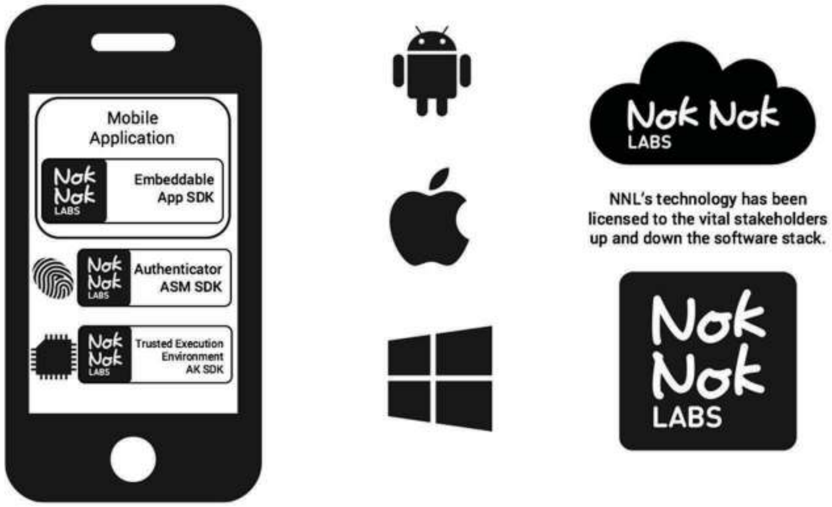
This framework boasts several advantages over passwords or other forms of authentication. Users are leveraging devices they already have – no new hardware is required. Therefore, the purchase and shipping of hardware tokens is unnecessary. This same device usually will boast a microphone, a camera, a fingerprint sensor – allowing the relying organization to leverage the growing wave of biometric technology already deployed in the market. The servers run by the organization are filled with cryptographic public keys – a mature and proven technology that has been shown to be lacking in value without the corresponding private key therefore it is not a target for malicious actors.

Strong authentication is about improving the number of signals an organization receives from an authentication event. After all, authentication is about a claim (I am John Doe) and a calculation (the likelihood of me being John Doe is X% because of Y). The more signals a relying organization can have, the higher confidence they will have that their calculation is correct. The protocol established by the FIDO Alliance creates a framework where multiple strong signals can be communicated to the relying organization through a trusted and secure channel. Of course, a framework is not a deployable technology. For that, the experts in FIDO implementation are needed. Enter Nok Nok Labs.

The Expert in Implementation

Our participation in the FIDO Alliance is no coincidence. The creation of FIDO happened in concert with the launch of Nok Nok Labs. We invented the initial protocol, performed the first deployment, performed the largest deployment, licensed its technology to the broadest range of device and component manufacturers and are the worlds' leading experts on FIDO.

Nok Nok Labs
Security from the Silicon to the Cloud



NNL's technology has been licensed to the vital stakeholders up and down the software stack.

The FIDO Alliance is an industry consortium where intellectual property has been pooled to solve the password problem. The initial set of patents and the protocol itself was invented at Nok Nok Labs. All the work that has been created since then has been based on the principles and policies first enshrined by our engineers. Since that time, Nok Nok has gone on to innovate and improve our core product. Nok Nok Labs has gained experience addressing the needs of multiple verticals from finance and banking to mobile network operators and healthcare. Nok Nok has built integrations into enterprise software and IoT products and our solutions are now capturing the interest of the entertainment industry and government services. There is not a company or firm in the world who can match the experience Nok Nok Labs has applying the FIDO protocol to as diverse a set of use cases and across as many market verticals.

A security chain is only as strong as its weakest link. That is why our solution provides assurances from the silicon to the cloud and every layer in-between. We license kernels of our technology to chipset manufactures to ensure that key generation and storage take place in secure and trusted elements on a device. Best-in-breed biometric authentication vendors come to Nok Nok Labs to elicit our assistance in building authenticators that maintain the secure, FIDO approved channel for the transmission of verified identity. Operating System vendors work with Nok Nok Labs to enable their systems to be able to securely encrypt and leverage the FIDO signals. Developers of mobile applications license Nok Nok Labs unique embeddable FIDO-client to allow their mobile application to leverage the entirety of the FIDO stack Nok Nok has put into place. The final step has been the on-going licensing and deployment of the Nok Nok Authentication Server that operates as the necessary FIDO component in the back end of an organization's software architecture – making sure they can field requests from 10 to 100 million or more users in a professional, responsive manner.

> With all this investment, there are simply no other company with as much experience up and down the FIDO stack as you find at Nok Nok Labs.

This expertise is not lost on the 260 (and growing) member organizations of the FIDO Alliance. Nok Nok Labs is the vendor of choice for various services that the alliance offers its members. Several times a year, companies from around the world meet to verify that the products they have built on the FIDO protocol are truly interoperable. Nok Nok Labs builds and operates the interoperability server that provides that verification. At last count, there were over 250 different products that had been checked and verified as interoperable using Nok Nok Labs technology. Additionally, the FIDO Alliance provides a metadata service which ensures that the various authenticators – who are constantly being improved and added to – are continually able to speak to FIDO servers. This service also runs on technology developed and provided by Nok Nok Labs.

The expertise at Nok Nok Labs goes beyond the standard FIDO specification. Due to this breadth and depth, engaging with Nok Nok means the technology an organization works with, the individuals they meet, can do far more than implementing the simple parameters of a written protocol. Nok Nok Labs has introduced out-of-band authentication, device blessing, multiple different risk signals for incorporating into fraud engines, policy editors for the server, and on
and on and on.

Nok Nok technical experts and business leaders have spoken at over 100 major conferences in the past 5 years.

The need for strong authentication is evident. The method to enact it is clear. The partner needed to ensure it is done well, done quickly, and done right has been argued for. The question remains: Why is now the time to act?

A Time of Convergence

Every wave of innovation in technology and services is followed by a wave of construction of infrastructure. The new technology ushers in new ways of doing things where the old ways no longer apply. In the past, passwords were sufficient when a user had only one or two services and those services were limited in what they offered and the cost of a breach was low. Today the average user has dozens of services while reusing the same password repeatedly. And these services are managing their money, their health records, even access to their homes. Yesterday's way of doing things just doesn't work for today.

Services have likewise moved to a mobile-first mentality deploying cloud hosted servers and leveraging the ubiquity of heterogeneous devices. Webpages are no longer being designed for siloed experiences between a mobile and desktop device – the omni-channel experience is the paramount design aesthetic.

These waves of innovation have arrived. Users expect an experience free from friction and free from cognitive-load. They desire an on-demand service, wherever they might be, using whatever device they have. To take full advantage of the potential these innovations have unleashed; it is now time to insure the infrastructure they are built on has the flexibility and resilience it needs.

There are over a billion devices in the market today that can support the FIDO protocol. Authentication technology has matured to the degree that users no longer need special training to be able to properly operate it. This same technology has proliferated massively and is incorporated into devices across the board. In fact, even for devices not initially shipped with a biometric authentication package, software based authenticators are available and small enough to be wrapped into a mobile application.

The threats and dangers of hosting server-side secrets are ever increasing. The costs for resetting and managing passwords are continuous and onerous. Authentication no longer needs to be a source of friction and the cause of lost revenue.
It can be a gateway to greater services, greater security, better customer experience and lower costs. Authentication can be strong. It can be simple. And it can scale to meet all your needs today and those you will build for tomorrow.

Strong Authentication: It is time to act.

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
4151 Middlefield Road, Suite 200
Palo Alto, CA 94303 USA

www.noknok.com

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

Nok Nok
LABS