THE NEXT GENERATION OF MOBILE AUTHENTICATION

Any device.
Any application.
Any authenticator.

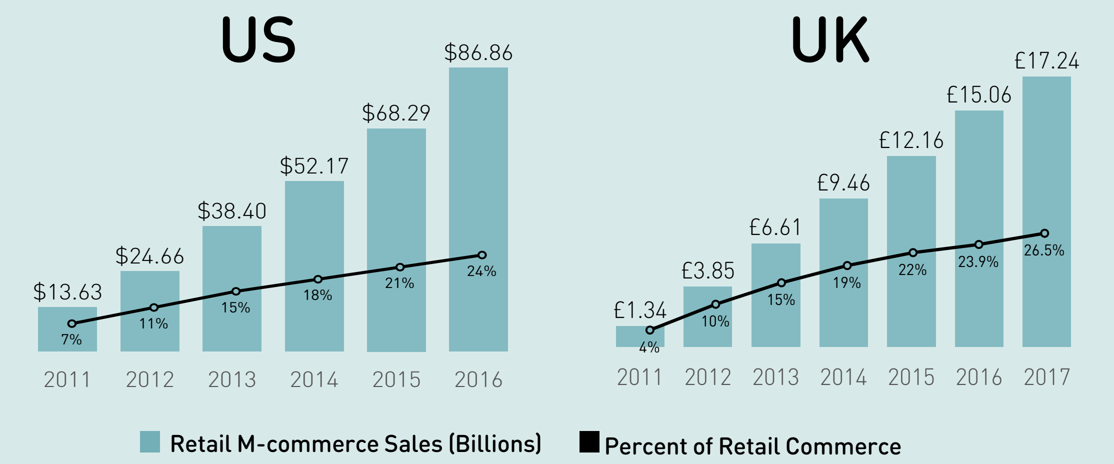
Nok Nok
LABS

TABLE OF CONTENTS

Nok Nok
LABS

INTRODUCTION

Figure 1
Forecast of US and UK Retail M-Commerce Sales



Note: Excludes travel and event ticket sales; includes sales on tablets.
Source: emarketer, 2013

It is not an exaggeration to say that our mobile devices have become an extension of ourselves. Users purchase products, book tickets, make dinner reservations, trade stocks, flag car rides, and perform a multitude of other transactions with their devices. These new forms of mobile commerce are growing at a dramatic rate, disrupting old markets and creating new ones. Innovative services and business models are emerging that take advantage of the always present and personal nature of mobile devices in order to enhance everyday transactions. Given the nascent state of mobile commerce, this trend is predicted to continue (Figure 1), and many more forms of mobile commerce will emerge in the future.

Transactions that formerly would have taken place in other domains are now moving to mobile. Users' preference for performing these transactions on mobile devices can be attributed to the convenience and ease of use these devices and applications provide. One example of applications that deliver convenience and ease of use is the "ridesharing" apps that are gaining wider adoption. These applications make it much easier for users to schedule a pickup and pay for a ride. Mobile ridesharing applications even charge the user automatically at the end of the ride, without requiring any action from the user such as swiping cards, counting bills, or calculating tips.

Removing such friction from the transaction has played a key role in the successful growth of mobile commerce. Removing friction requires mobile commerce apps and services to manage the risk of user impersonation and/or verify that the person executing the transaction is the legitimate owner of the device and the account. Some transactions may involve little marginal risk, so the app may simply trust that the device is in the right hands. However, other transactions, such as mobile banking and app store purchases, can involve higher degrees of risk and may require explicit verification steps. Such applications use diverse authentication methods to verify the user. For this class of applications, authentication is essential to enabling mobile commerce.

USABILITY AND AUTHENTICATION

Design and user experience are critical competitive dimensions in the mobile world and often seem to be the deciding factor between failure and success for competing apps. In this world, a flaw in a single step of the user's flow can affect the success of the entire app. A poor authentication experience can introduce tremendous friction at the moment the transaction is being completed. This diminishes the convenience value proposition of mobile commerce, reducing both user engagement and transaction completion rates.

While many aspects of the mobile user experience have seen significant innovation, the authentication experience on mobile devices has not kept up. Most efforts related to mobile authentication involve applying mechanisms used in the desktop world to the mobile world. However, many mechanisms designed for desktops have proven to be a poor fit for the mobile form factor. For example, although passwords are easy to enter on the full-size keyboard of a laptop, they are challenging and error-prone to enter using the small keyboards on mobile devices. Further, many applications have password policies that require a combination of letters, numbers, and even special characters. These policies can be particularly troublesome on mobile devices, requiring users to switch between multiple touchscreen keyboard modes to enter the required password.

The usability problem is even worse for many strong authentication mechanisms. For example, one-time passwords (OTPs) used by many applications compound the text entry problems of passwords. OTPs require the transfer of text from either another application or an SMS message. This forces the user to switch back and forth between applications while performing either copy-and-paste or text entry, increasing the possibility of user errors and frustration. Many other strong authentication methods, such as smartcards and USB tokens, do not interoperate with mobile devices due to the lack of compatible readers or ports. It is clear that a convenient authentication user experience for mobile devices has yet to be delivered.

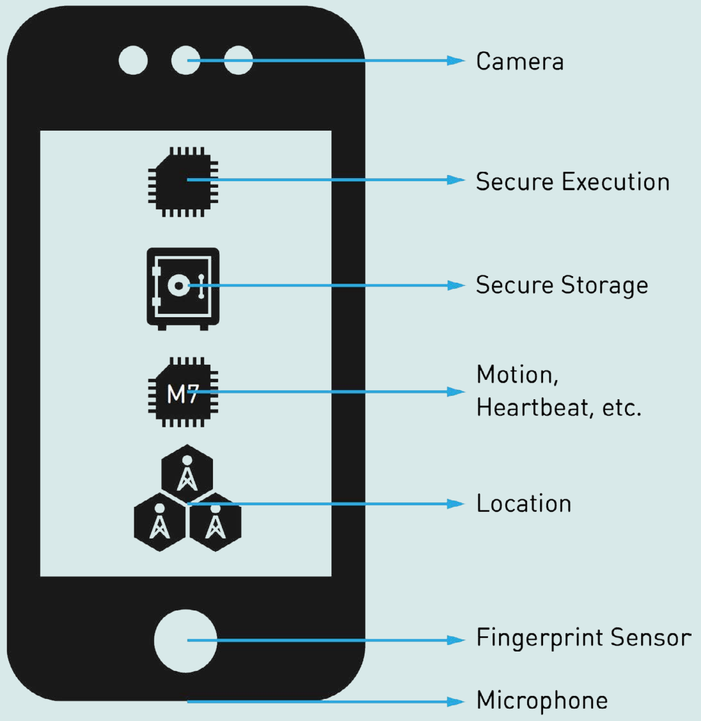
THE NEXT GENERATION OF MOBILE AUTHENTICATION

Many mobile devices already include technology building blocks that could be used to provide the next generation of user-friendly strong authentication to applications running on-device (Figure 2). These technologies can be used to remove friction, improving transaction completion rates and user satisfaction. Mobile devices are equipped with a growing number of sensors that can ease the pain of authentication. For example, smartphones and tablets feature powerful cameras and sensitive microphones that can be used for biometric authentication. Higher-end devices and some newer devices are equipped with fingerprint sensor technology.

Technologies that are built into mobile devices improve not only explicit authentication (which requires the user to perform actions) but also implicit authentication (which automatically occurs on the server without any effort by the user, such as a risk-based fraud system). On-device sensors—such as GPS chips, temperature sensors, humidity sensors, barometers, and accelerometers—can be used to augment explicit authentication with implicit or risk-based authentication (RBA) techniques. Even the WiFi interface can play a role in determining whether the user is possibly being impersonated by an attacker.

Mobile devices themselves can act as a token to authenticate to off-device applications and services. Such devices include several short-range communication interfaces—such as WiFi, Bluetooth low energy (BLE), and near field communication (NFC)—that can be used to securely provide authentication credentials to other applications. For example, a user wishing to withdraw money at an ATM could authenticate to the bank and set up the transaction on a mobile device while waiting in line. The user could then execute the transaction by simply tapping the device on the ATM or clicking a button on the device. This action securely transfers the user's credentials and transaction information to the ATM, allowing fast and easy processing of the transaction. Such designs are already being field tested by ATM manufacturers. With the ability to securely authenticate users, mobile devices potentially can replace keys, wallets, and other objects that users have needed to carry with them.

Figure 2
Building Blocks for Authentication



SECURITY ADVANTAGES OF THE MOBILE PLATFORM

Mobile devices can not only improve usability but also provide more secure authentication. This reduces the risk of fraud and increases user trust in the business. Devices feature powerful multicore processors and gigabytes of memory, enabling the use of computation-intensive cryptography, complex biometric algorithms, and heuristics. Mobile devices can even exceed the security of PCs in many areas. Many mobile platforms tightly regulate the user's ability to install apps on devices through app stores, limiting the risk of malware. Most mobile operating systems restrict the mechanisms used by applications to communicate with each other, thereby limiting the ability of malware to access data from legitimate applications. Mobile operating systems also include a host of security features, such as encrypted storage, per-app VPNs, remote wipe, and cloud-based password managers.

Mobile devices also offer secure hardware capabilities that can be used to strengthen authentication software. Some subscriber identity module (SIM) and Secure Digital (SD) cards incorporate chips called secure elements (SEs), which provide hardware-level support for security capabilities such as encryption, cryptographic key generation, and secure storage. Many manufacturers have long embedded SEs in the devices, allowing some applications to take advantage of the available security capabilities. A more advanced security capability emerging on mobile devices is the Trusted Execution Environment (TEE), based on ARM TrustZone® technology. The TEE is essentially a secure execution mode incorporated into mobile processors that creates a secure barrier between trusted and untrusted code. TEEs also include mechanisms to ensure that only authorized or trusted code can be run within them. This mode can protect large portions of applications and system software from modifications or access by malware. The architecture of mobile platforms, combined with the emerging secure hardware capabilities, provides the foundation for more secure and usable authentication on mobile devices.

THE MOBILE AUTHENTICATION CHALLENGE

Although today's devices are rich in the technological building blocks for strong authentication, organizations have few, if any, mechanisms to take advantage of those technologies for mobile authentication. Smartphones may ship with cameras, but few include face biometric software. Even those that do ship with face recognition capabilities limit their use to screen unlock. There are no interfaces that allow a third-party application to use these built-in capabilities. For example, it is not possible for a user to authenticate to eBay using his smartphone's camera. The necessary interfaces, standards, and integrations that would solve the authentication problem have not been available.

A second problem related to strong authentication on mobile devices is caused by fragmentation. Decades ago, the PC world rallied around a single de facto standard—the Wintel platform—making it easy for applications to interoperate with the PC ecosystem. However, in the mobile world there is no such de facto standard. The mobile ecosystem is highly fragmented, with multiple operating systems (and even multiple flavors of the same operating system) and widely varying device capabilities. Devices differ in processing power, memory, camera resolution, secure hardware capabilities, presence or absence of fingerprint sensors, and many other features and aspects. Further, the landscape is constantly changing, with mobile users typically upgrading their devices at least every two years. The fast pace of new innovations, combined with the short upgrade cycles, creates tremendous interoperability problems in the mobile ecosystem.

For any mobile application, supporting a large user population with a wide range of devices can quickly become an intractable problem. Historically, authentication systems have been architected primarily for the static, homogeneous PC world. A typical authentication system is built using proprietary components to address a specific set of use cases or scenarios. As the diversity of devices and use cases increases, organizations add on new authentication systems to address their broader user base. Frequently built by different vendors, these systems do not interoperate or communicate with each other ; in essence, they operate as authentication silos. These architectural silos result in great complexity, cost, and redundancy for organizations. Further, this approach results in a very brittle architecture, limiting organizations' ability to respond to changes in the authentication landscape such as availability of new authentication mechanisms or discovery of vulnerabilities in existing mechanisms.

MOBILE AUTHENTICATION STANDARDS

Recently there has been an effort to meet the need for mobile authentication standards. Standardization helps applications, devices, and authentication mechanisms to interoperate with each other, thereby reducing cost, complexity, and risk for mobile authentication deployments. Standardization allows vendors to bring new authentication innovations to market faster, so the authentication experience can keep pace with innovations in other aspects of mobile devices. An important standardization effort emerging in the mobile space is being championed by the Fast IDentity Online (FIDO) Alliance.*

Fast IDentity Online (FIDO) Alliance

The FIDO Alliance is an industry initiative working to create standards that address the interoperability problem among devices, applications, and authentication mechanisms. FIDO standards will allow organizations to deploy a unified authentication infrastructure and support any authentication method on any device. In effect, FIDO unifies current authentication silos with an agile and simplified architecture. The FIDO architecture reduces the cost and complexity of deploying authentication and future-proofs organizations, enabling them to easily support new devices and authentication technologies.

FIDO is not a third-party service or a separate proprietary approach to the authentication problem. FIDO standardizes a generic authentication protocol, allowing devices to interoperate with different authentication methods. The FIDO architecture decouples applications from the details of each authentication method and allows applications to support virtually any authentication method on those devices that implement the protocol, using a single integration.

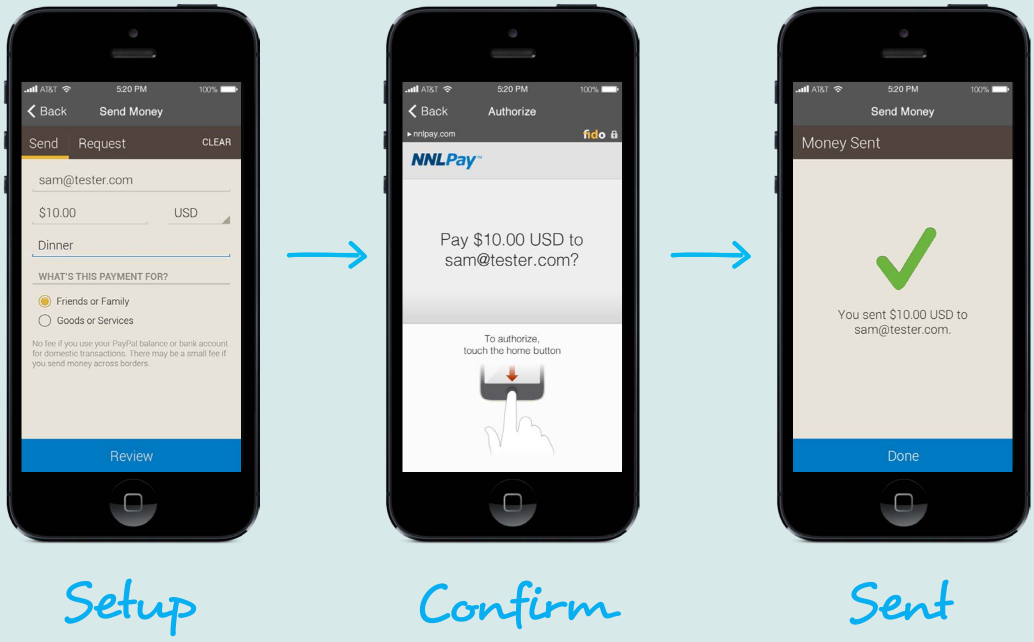
* See www.fidoalliance.org.

Devices implementing FIDO protocols can take advantage of native capabilities such as cameras, microphones, TEEs, SEs, and other technologies to provide authentication that is both more user-friendly and more secure than a password. Users can authenticate to applications using their existing mobile devices with a wide variety of easy-to-use methods, such as face recognition, voice recognition, PINs, and many others. FIDO protocols use public key cryptography to improve the security of authentication while simplifying the authentication implementation server-side. FIDO currently supports authentication for browser-based and mobile applications.

Based on need, applications can set policies specifying which authentication methods are acceptable. The FIDO protocol allows users to enroll themselves with the application using one or more of the specified methods. Applications can require additional authentication based on the risk involved in the transaction. For example, a user transferring $10,000 may be required by the relying party to authenticate using both face and voice recognition to obtain a higher level of assurance. The flexibility provided by FIDO also future-proofs applications, as support for newer authentication mechanisms can be enabled by simply making policy changes.

The FIDO protocol greatly improves the authentication user experience (Figure 3). For example, a user who purchases a FIDO-enabled phone with a fingerprint sensor can enroll her fingerprint with the device when first activating the device. During this enrollment, the user swipes (or presses) her finger on the sensor until a usable sample is obtained. Later, when authenticating to a mobile payments application, for example, the user is presented with an option of using the fingerprint sensor for future logins. The user can accept and register with the application by simply swiping (or pressing) her finger once. When the user accesses the application in the future, she simply logs in with a finger swipe, with no need to type a username or password. Similarly, the device can also be used to authenticate to desktop applications using a fingerprint sensor. In this scenario, the mobile device authenticates the user by verifying her fingerprint and communicates authentication credentials using an interface such as Bluetooth LE, allowing the desktop application to log the user in. In all cases, the fingerprint biometric data is stored securely on the device and is only used for local fingerprint matching algorithms. The biometric data is never transmitted externally to other devices or servers.

Figure 3
The FIDO User Experience



sam@tester.com
$10.00 USD
Dinner
WHAT'S THIS PAYMENT FOR?
● Friends or Family
○ Goods or Services
No fee if you use your PayPal balance or bank account for domestic transactions. There may be a small fee if you send money across borders.

Pay $10.00 USD to sam@tester.com?

To authorize, touch the home button

You sent $10.00 USD to sam@tester.com.

CONCLUSION

Mobile platforms are greatly expanding opportunities in mobile commerce by removing friction from transactions. To make transactions smoother, mobile applications rely on being able to trust the user's identity at all times, in many cases through authentication. Although many aspects of the mobile user experience have significantly improved, the authentication user experience has not kept up. Most activities in mobile authentication have relied on porting authentication mechanisms built for the desktop to mobile devices. However, many of these mechanisms, such as passwords and hardware tokens, have proven to be a poor fit for mobile devices.

Today's mobile devices are powerful platforms offering a wide range of capabilities that can be used to provide more secure and usable authentication suited for mobile devices. Cameras, microphones, secure hardware, and other capabilities could be leveraged to enable authentication mechanisms such as face and voice recognition. However, the standards and integrations necessary for wide adoption of such mechanisms have not been available.

FIDO is a standardization effort to address this gap in mobile authentication. FIDO enables interoperability among devices, applications, and authentication mechanisms, using an extensible authentication protocol. Standardization unifies proprietary authentication silos, thereby reducing cost and complexity while improving the user experience and security of authentication. FIDO allows organizations to implement a single flexible, unified authentication infrastructure to serve all their authentication needs. The result is:

- An improved, more secure user experience
- More innovation in current and future authentication methods and technologies
- Increased growth with decreased costs for companies whose systems rely on user authentication.

Nok Nok Labs' Multifactor Authentication Server (MFAS) and Multifactor Authentication Client (MFAC) are end point implementations of FIDO protocols.

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 mission 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

Nok Nok Labs, Nok Nok, and NNL are all trademarks of Nok Nok Labs, Inc.

FIDO is a trademark of the Fast IDentity (FIDO) Online Alliance.

© 2013 Nok Nok Labs, Inc. All rights reserved.