Biometrics in Banking

How to Integrate Touch ID into your Mobile Banking Application the Right Way
| Introduction | 1 |
| Adoption of Touch ID as a banking authentication tool | 2 |
| Touch ID: Benefits to deployment and the risks of doing so incorrectly | 4 |
| Merits of VASCO’s DIGIPASS for APPs solution, which helps institutions reap the security benefits of Touch ID | 8 |
Introduction

Banks can no longer view mobile banking as a “new channel” or optional service. It is now the preferred form of banking for an entire generation of customers and, arguably, the single biggest banking innovation since the advent of the ATM.

Biometrics - specifically the use of fingerprints, iris scans and facial recognition as a means of authentication - increasingly has become an accepted part of daily life. Several governments, including the United States, Canada and United Kingdom, have adopted biometrics, as the technology continues to improve.

In 2013, Apple introduced Touch ID, a fingerprint scanning technology embedded in the company’s new (at the time) iPhone 5s. Touch ID signaled the beginning of a new era by bringing convenient fingerprint recognition to a mass consumer audience. In addition, Apple supplied third parties with Touch ID APIs, so that outside developers could integrate the technology into their own apps and services.

Banks in particular have gravitated to Touch ID technology because it provides them with a device-based technology they may leverage to secure the mobile banking platform, and, in turn reduce their costs in deploying and supporting such services. At the same time, however, banks face the challenge of integrating this biometric technology within their security architecture while avoiding unforeseen security risks.

This report discusses:
- Adoption of Touch ID as a banking authentication tool;
- Benefits of Touch ID, as well as the risks of deploying it incorrectly; and
- Merits of VASCO’s DIGIPASS for APPs solution, which helps institutions reap the security benefits of Touch ID.
Adoption of Touch ID as a banking authentication tool

When mobile banking first arrived, banks often limited their services. While the availability, functionality and ease of use compelled customers to embrace mobile devices, banks initially viewed mobile platforms as inherently insecure. Consequently, many banks prevented the deployment of high-value services via mobile banking. Certain financial institutions allowed customers to check balances, while others applied limits to fund transfers, but few offered the array of services available online for PCs.

While banks possessed the technical capabilities to support a fully functional mobile banking platform, they could not secure the channel sufficiently to provide secure services such as opening new accounts, higher limit fund transfers or third-party payments via P2P. The convenience of mobile devices only underscored the ease in which one could be lost or stolen - and banks weren’t willing to make their most sensitive information readily available to criminals.

Before Touch ID banks resisted using biometric technologies, such as fingerprint-based authentication, because such technologies were difficult, if not impossible, to implement on mobile devices. Al Pascual, director of fraud and security at Javelin Strategy and Research, says that banking institutions have long expressed an interest in biometrics as a method to authenticate customers. However, finding cost-effective solutions have proved challenging in general.

“Touch ID provides a way for financial institutions to deliver authentication at a negligible cost.”

Al Pascual, Director of fraud and security at Javelin Strategy and Research
But Apple’s innovation revolutionized mobile device security by providing a painless way for users to secure their iOS devices and supplying third-party developers with the APIs to integrate it into their own apps. Thanks to Touch ID, financial institutions now had access to a commonly available and convenient technology to authenticate mobile customers.

Pascual, for his part, sees tremendous benefits to banks. “Touch ID provides a way for financial institutions to deliver authentication at a negligible cost. You do not have to pay Apple to gain access to Touch ID. It is free, in a manner of speaking, because Apple incurred the software development costs and it is available to developers. That’s a huge differentiator when compared to biometrics of the past,” he explains.

Banks view biometrics as more secure than simple passwords, while customers embrace their simplicity and convenience. If integrated incorrectly, however, Touch ID can weaken a financial institution’s security-related defenses and heighten the level of financial, operational and reputational risk associated with the mobile banking platform.
Touch ID: Benefits to deployment and the risks of doing so incorrectly

Why choose Touch ID?

Matthias Valcke, Business Solutions Manager with VASCO Data Security, knows first-hand what banks expect when it comes to authenticating their mobile customers.

Banks worry about mobile device security. “They want to implement mobile security, but it needs to be convenient. Customers will not accept inconvenient security solutions. There is a big push from the business people to make mobile banking quick and convenient,” Valcke says.

Valcke sees secure mobile banking as the best way to facilitate the inevitable customer-driven push toward mobile banking. “The more you make the mobile platform secure, the easier it is for the bank to offer more functionality to customers,” he says. “Increasing the trust level in the mobile app and, by extension, the mobile platform allows banks to close the gap between mobile banking and Internet banking.”

In addition to authenticating users, Valcke believes that implementing Touch ID gives banks a way to differentiate their services in an increasingly crowded marketplace. When banks adopt Apple’s fingerprint reader as an authentication method, they delight customers with its ease of use - and motivate them to use it as a primary channel.

“Increasing the trust level in the mobile app and, by extension, the mobile platform allows banks to close the gap between mobile banking and Internet banking.”

Matthias Valcke, Business Solutions Manager at VASCO Data Security
Pitfalls of integrating Touch ID

At the same time, this push to quickly adopt Touch ID led some banks to implement it in ways that were inherently insecure. “When they created Touch ID, Apple went one step further and linked it to their Keychain,” Valcke says. “Basically, it means that as an app developer, if you create an app, you can store something in Keychain, and every time you need that data from Keychain, the user is forced to use the same fingerprint. Only then can the app access that data.”

Keychain, a password management system developed by Apple, allows for the storage and access of data, typically protected by the user’s regular login password. Employed in this fashion, however, Keychain cannot provide the level of authentication banks need within the mobile channel. Using just a fingerprint by itself provides local authentication. But as Valcke points out, banks require remote authentication.

By storing server passwords in Keychain, developers can convert local authentication into a remote authentication system. Storing a static password on user’s device using Keychain allows the customer to authenticate via Touch ID and avoid manually entering his or her password. Once the customer authenticates his or her identity, the mobile app retrieves a server password from Keychain and delivers it to the bank’s server.
4 Challenges of integrating Touch ID into your banking application

1 Risks of storing server passwords locally

But storing user passwords on their devices introduces a new set of problems banks often overlook in their rush to embrace Touch ID. In the event that a user device is lost, stolen or jailbroken, that device’s Touch ID password may end up in the possession of third parties intent on committing fraud. Similar to locking a desk drawer and the lock malfunctioning, a device with a compromised operating system can grant third-party access to Keychain, and therefore, the bank’s server and customer’s account.

Despite consumer confidence that a fingerprint provides an unimpeachable form of security, user passwords, should they remain in static form, remain an area of vulnerability. The potential for unauthorized access is only compounded when customers reuse their passwords. Further, if a breach occurs because of a flawed implementation of Touch ID, customers may lose confidence in Touch ID and their bank. This possibility of losing customer mindshare in this manner is a particular challenge for financial institutions.

2 Linking fingerprint to an unsecured static password

To complicate matters, consumers often own multiple devices, from smartphones and tablets to car-borne Internet browsers, such as Tesla’s vehicle platform. But when a user changes his or her mobile banking password on, say, a work iPhone, that password does not update automatically on the user’s other mobile devices. When this user attempts to access mobile banking via a second personal device, that device cannot authenticate the login, as it cannot access the new, yet static password stored within the other device’s Keychain.

3 Multi-device synchronization
While customers understand they must assume some level of responsibility for protecting their personal information, as well as their mobile banking login credentials, few understand how to do so, especially in context of Touch ID, which too many view as hacker-proof. Customers face additional risks should they jailbreak their mobile devices, lose them or return them to a company or provider without thinking to wipe their personal data. Consequently, banks must step in to assume some of the security responsibility, if only to save customers from themselves.

4 Lack of device control by the bank

Risks of storing passwords locally
Linking fingerprint to an unsecure static password
Multi-device synchronization
Lack of device control by the bank
Merits of VASCO’s DIGIPASS for APPs solution, which helps institutions reap the security benefits of Touch ID

Authenticating mobile customers in an efficient and effective manner requires the intelligent deployment of technology. When financial institutions deploy Touch ID in a way that removes server passwords from user devices, they significantly reduce the risk of compromise.

While banks recognize that mobile customer authentication requires local and remote authentication, how they verify a customer’s identity requires leveraging Touch ID while avoiding the aspects of this biometric technology that embed an inherently flawed approach to security.

Notwithstanding that Touch ID allows banks to perform local authentication using a fingerprint reader and remote authentication using passwords stored in the device’s Keychain, adopting such an approach creates significant risk.

VASCO’s DIGIPASS for APPs solution establishes a secure bridge between local authentication (what a user expects) and remote authentication (what a bank requires).

Enhanced Security and a Transparent User Experience

VASCO’s DIGIPASS for APPs solution establishes a secure bridge between local authentication (what a user expects) and remote authentication (what a bank requires).

It offers developers a rigorous security feature-set that they may integrate into their mobile banking apps, using a combination of:

- Multifactor authentication
- Integration with biometrics, such as Touch ID
- Jailbreak and Rootkit detection
- Secure storage
- Geolocation
- Device binding
- Risk based scoring
- Secure communication
- App shielding through Runtime Application Self Protection (RASP)
How it works?

Instead of storing a static password on a user’s device, upon local authentication, the device retrieves an unlock key stored within Keychain. This key is one of the required parameters to generate a one-time password for server authentication.

“The cryptographic key to generate one-time passwords is constructed on the fly, using data in the Keychain (unlocked with fingerprint), unique information on the phone and VASCO’s secure storage inside the application,” Valcke points out. This approach also inserts a platform fingerprint and platform security score within the authentication code. This allows the server to check:

- If authentication is successful
- If the request is coming from a known device
- The security/risk level of the device. Is the device jailbroken, for example?
Conclusion

By using DIGIPASS for APPS, banks can implement local and remote authentication, without the need to manage a user’s passwords. Since there is no shared data and no synchronizing needed between devices, a lost or compromised device does not impact other devices. Ultimately, this creates a frictionless user experience and, because of the higher level of security and trust it engenders, a secure environment for banks to deploy additional services via their mobile banking applications.

Download the ‘Increasing Business with Mobile Banking’ security ebook:

www.vasco.com/MobileBanking
About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

About iSMG

iSMG is the largest media company solely focused on Information Security, Risk Management, Fraud, Compliance and other related topics. The firm’s footprint and the subscriber-base extends from the North American markets to Europe, Asia and Australia.

Learn more about iSMG at www.ismgcorp.com