Entersekt

SECURING THE MOBILE BANKING CHANNEL

Many banking customers doubt the security of the mobile banking channel. Current solutions to digital fraud have failed to alleviate this unease and have had a negative impact on the user experience. Mobile malware, meanwhile, is fast on the rise, threatening to make the situation worse. If banks want to protect their customers from account takeover fraud and secure their future in a disrupted marketplace, they must innovate. Intelligently reengineering user and transaction authentication on the mobile channel is the first, crucial step on that path.

The mobile opportunity

That the world has enthusiastically embraced mobile technology goes without saying, but mobile really has been enormously transformative. Within a few short years, mobile applications have become an indispensable feature of daily life, serving as sources of information, productivity tools or entertaining ways to pass the time. There are now almost 1.4 million Android apps on the market and nearly as many available to users of Apple's mobile devices.[1][2] By October 2014, 85 billion apps had been downloaded from the Apple App Store.[3]

To their credit, financial services companies moved quickly to tap the potential of this channel, rolling out functional, albeit basic, mobile banking apps. Many of their retail banking customers have shown their appreciation, signing up for time-saving convenience and accessibility. According to the *2014 Consumers and Mobile Financial Services* report by the Board of Governors of the Federal Reserve System, released in March 2014, approximately 33 percent of all mobile phone owners in the USA had used mobile banking in the past 12 months, up from 28 percent a year earlier. Of smartphone owners, nearly 51 percent had used mobile banking in the past 12 months, up from 48 percent.[4]

On the other hand, doubts over mobile security have kept a sizeable percentage of consumers from taking up mobile banking. Security concerns have also caused banks themselves to delay offering a full range of financial services through the channel. This is especially true for high-value, high-risk transactions, such as wire transfers, ACH or stock trading.

For financial institutions to prosper in the mobile era, building trust in the mobile channel is imperative. Security cannot, however, compromise usability, not without turning customers away. Ease of use, or the lack of it, is another important factor hindering adoption, as countless surveys indicate.

Competition is tougher than ever before in a marketplace attracting an array of non-traditional banking and payments providers. Complacency is extremely dangerous. There has never been a more important time for financial institutions to differentiate themselves through technological innovation. They must demonstrate their responsiveness to their customers' concerns and engineer positive mobile banking experiences that balance the seemingly opposing goals of heightened security and convenient access. Their customers will reward them for their efforts. The financial services companies of tomorrow are those that grasp the mobile opportunity today.

Threats to mobile security

Insufficient oversight of a fast evolving ecosystem

In 2005, the FFIEC (Federal Financial Institutions Examination Council) issued *Authentication in an Internet Banking Environment*, its initial guidance to US financial institutions on providing effective user identity authentication online. A supplement followed in 2011, updating "expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment." The supplement was welcome, but did not address authentication and identification controls on mobile. There is just one reference to a "telephone".[5]

The Anti-Phishing Working Group is a global consortium of financial services companies, service and technology providers and law enforcement agencies dedicated to fighting digital fraud and identity theft. Its chairman is David Jevans, founder of and Chief Technology Officer at Marble Security. He sums up the situation succinctly:

> "For some time, the FFIEC has said that, depending on the risk of a transaction, two-factor authentication is required. The U.S. banking industry is moving fairly rapidly to using mobile phones as a two-factor authentication device. The problem is that mobile is now the platform of choice for online banking, not PCs, so banks are asking for guidance on two-factor authentication for mobile banking. If people are banking via mobile devices and they get authentication codes sent via SMS to their mobile device, they aren't getting any extra security. The risk is that the mobile device may have been compromised."[6]

There has been speculation that the FFIEC will issue guidance in this area very soon; hopefully it does so. In the meantime, other bodies have stepped into the breach. In 2013, BITS, the technology policy arm of Washington, D.C.–based Financial Services Roundtable, released the *BITS Mobile Technology – Layered Security Model*, "an evaluation of mobile-specific security threats and an identification of mitigating controls."[7] The Financial Services Information Sharing and Analysis Center (FS-ISAC), a global financial services cyber-security forum, has also developed guidelines for US community banks that address aspects of mobile banking security.

With all new technologies, establishing and maintaining rigorous standards helps build consumer confidence and drive mass market acceptance. This is particularly true where user safety is a factor. The proliferation of mobile banking services, along with the inevitable rise in mobile malware in the last couple of years, points to mobile security standards necessarily becoming a top priority for regulators.

Poor app design and configuration

Mobile banking apps tend to be safer than banking using a mobile browser, but a growing number of data breaches and security incidents can be linked directly to poor code quality in banking apps. Securing mobile involves navigating a labyrinth of handset manufacturers, mobile operating system developers, app developers, mobile carriers and service providers. Every mobile platform has its own quirks that developers must accommodate, and each device presents a unique set of challenges to overcome. Mobile app developers do not always adequately understand the risks that proliferate in this extremely complex ecosystem and most, sadly, are not up to the task of securing mobile data, connections and transactions.

Securing mobile involves navigating a labyrinth of handset manufacturers, mobile operating system developers, app developers, mobile carriers and service providers.

Even if they possess the necessary knowledge, developers often lack the resources or the time to properly protect users of their apps and the systems with which they interact. Four out of five IT security professionals surveyed in Trustwave's global *2014 Security Pressures Report* indicated feeling pressure to roll out projects despite their own unaddressed security concerns.[8]

"So long as IT organizations sacrifice software quality and security for the sake of meeting unrealistic schedules, we can expect to see more high-profile attacks leading to the exposure and exploitation of sensitive customer data," says Lev Lesokhin, Executive Vice President of CAST, which analyzes software for security risks on behalf of large financial services companies. "Businesses handling customer financial information have a responsibility to improve software quality and reduce the operational risk of their applications – not only to protect their businesses, but ultimately their customers."[9]

According to CAST, finance and retail industry applications are the most vulnerable to data breaches, with 69 percent of financial services applications shown to have data input validation violations. In January 2014, cybersecurity firm, IOActive, made global headlines when it reported manifold security flaws in 40 mobile banking apps from among the 60 most influential banks in the world.[10] Ninety percent of the apps used non-SSL links. Half were vulnerable to JavaScript injections. Forty percent were susceptible to basic man-in-the-middle attacks, in part no doubt because 70 percent did not provide "alternative authentication solutions, such as multi-factor authentication, which could help to mitigate the risk of impersonation attacks."

In late 2013, researchers at information security firm, Praetorian, painted a similar picture after testing 275 banking apps from 50 of the largest US banks, 50 large regional banks and 50 large credit unions. Praetorian described its testing as “not intrusive”, but nonetheless found eight out of 10 apps were not optimally configured or built using common fraud mitigation functions. To Praetorian, the large numbers of issues suggested that the roll-out of most banking apps had been rushed and that structural flaws, low risk but exploitable, had not subsequently been cleaned up.[11]

In an analyst brief released by NSS Labs around the same time, the author, Ken Baylor, also drew attention to the elementary security of banking apps brought quickly to market: “Most banks began offering mobile services with a simple redirect to a mobile site (with limited functionality) upon detection of the smartphone HTTP headers. Others created mobile apps with HTML wrappers for a better user experience and more functionality. As yet, only a few have built secure native apps for each platform.” Baylor – who is now Chief Information Security Officer at Pivotal, the big data and cloud computing joint venture between EMC Corporation and VMware – urges financial institutions to replace HTML wrapper apps with secure native mobile apps featuring hardened browsers, certificate-based identification, unique install keys, in-app encryption and more.[12]

Mobile malware’s explosive rise

Mobile malware often takes advantage of software bugs and vulnerabilities, so for hackers and cybercrime syndicates the present situation is approaching something of a gold rush, one that they are doing everything to exploit with thousands of new mobile banking trojans and hundreds of thousands of other malicious programs.

The two most popular smartphone operating systems are Android and Apple’s iOS. Android is by far the more widely used of the two and a much more open operating environment, allowing users to download apps from app stores that have less stringent analysis and vetting procedures. By contrast, iOS does not allow users to download apps from outside of the Apple App Store, which has a strict process for reviewing apps to eliminate the possibility of malware. Apple also does not permit customization of the iOS system to the extent that Google does with Android apps.

It’s no surprise then that Android users are most at risk from mobile malware. According to Trend Micro, more than a million malicious Android apps were discovered in 2013, bringing the total to 1.4 million and illustrating perfectly the exponential growth of this kind of vector. The software security company predicts malicious and high-risk Android app volume to reach three million by the end of 2014.[13] Kaspersky Lab says that 98 percent of all malware it detected in 2013 targeted the Android platform. Over the course of that year, the number of known *banking* trojans grew from 67 to 1321 unique instances, the company said.[14]

Most mobile banking malware is a variation on the theme set by Zeus-in-the-Mobile (Zitmo), the original SMS-stealing trojan. In 2012, one of the most successful Zeus variants, Eurograbber,

infected more than 30,000 users at about 30 banks in Europe and was used to steal an estimated €36 million ($45 million). Malware like this bypasses two-factor authentication systems by gathering SMS one-time passwords (OTPs) or intercepting and redirecting calls. Other malware steals user credentials through keylogging or screenshots. A Korean malware, Wroba, uninstalls legitimate banking apps and replaces them with counterfeits designed to harvest usernames and passwords.

Fake apps or hacked apps are also a growing problem. Examples have been found in reputable app stores, although consumers are obviously at greater risk downloading apps from unofficial app stores. Those that opt to "jailbreak" or "root" their mobile devices, enabling them to install software without restriction, also do themselves no favors. This practice removes safeguards from the device, leaving it more susceptible to attack. Some banks disable most mobile banking features on a rooted device, if they are able to detect it, which is increasingly difficult to do.

Operating systems' cryptographic vulnerabilities

"A common weakness found in mobile banking apps is that they lack adequate implementation of SSL or certificate validation, which makes them vulnerable," says David Jevans, Chief Technology Officer at Marble Security.[15] SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are the most important digital security protocols in use today, used to establish encrypted links between computers and servers and to ensure that any server is what it purports to be, thus helping to prevent phishing and man-in-the-middle attacks.

SSL does, however, fall prey to attack in certain situations. Chad Brubaker, an Android security engineer at Google explains: "Most platforms and devices have secure defaults, but some applications and libraries override the defaults for the worse, and in some instances we've seen platforms make mistakes as well. As applications get more complex, connect to more services, and use more third party libraries, it becomes easier to introduce these types of mistakes."[16]

Researchers say thousands of mobile apps across all mobile platforms do not adequately validate digital certificates.

Researchers say thousands of mobile apps across all mobile platforms do not adequately validate digital certificates, accepting either any certificate transmitted to them (self-signed ones included) or certificates issued for domain names different to those to which they were connecting. Researchers from Stanford University and the University of Texas Austin concluded in 2012 that "SSL certificate validation is completely broken in many critical software applications and libraries."[17]

A serious vulnerability in the popular OpenSSL cryptographic software library was discovered in 2014. Dubbed Heartbleed, it triggered panic across the Internet and set off an unprecedented patching effort. Several serious bugs have since been found in other SSL libraries.

The weakness of mobile device ID

Mobile devices – especially iPhones – share an important characteristic: they are very hard to tell apart. The problem is not so much their physical appearance as their weak "device fingerprint". Device fingerprinting involves gathering information about a remote computing device in order to identify it uniquely. Once fingerprinted and added to a database, the device can be recognized in the future for a wide range of purposes, including preventing fraud.

Some enterprises attempt to identify mobile devices in this way, combining characteristics like the IMEI (international mobile equipment identity) number, mobile number, and so forth. Concerns over privacy have, however, limited the amount of data shared by phones and tablets, meaning that there are not enough discrete data points to establish a reliable digital fingerprint of an individual mobile device. This effectively disqualifies device fingerprinting as a means of providing two-factor authentication or as a source of dependable behavioral analytics on the mobile channel. Gartner has stated that "solutions that worked well to identify user PCs, such as device fingerprinting, are not nearly as effective for mobile applications, so enterprises need to compensate and rely on other fraud-prevention techniques."[18]

Flawed authentication

As with online banking, mobile banking fraud centers on fraudsters' attempts to obtain confidential login information – including passwords, PINs and token codes – to gain access to accounts. To stay ahead of the cybercriminals, banks must reliably authenticate users accessing the mobile channel.

Two-factor authentication in online and mobile banking has typically relied on the one-time password (OTP), a single-use string of alphanumeric characters delivered to the user via a hardware token or text message. A fact of life for millions of bank customers globally, OTPs have never been popular. Users find having to carry OTP hardware a hassle and reentering the codes at login and for every subsequent transaction a clumsy, error-prone waste of time. This is especially true of mobile users, who must battle with small screens and tricky keypads.

More importantly, OTPs are no guarantee of protection from phishing attacks and malware-enabled account takeover fraud, as a decade of failure at the fingertips of cybercriminals demonstrates. From Swedish Internet bank, Nordea, in 2005, to Operation Emmental, which successfully targeted online banking accounts at over 30 banks in Europe and Japan in 2014, OTP-based authentication has succumbed to phishing attacks because it relies on browser communications back to bank servers. If a phishing site mimics a bank's online or mobile banking portal or the browser is otherwise compromised, the customer's credentials and the OTP can be harvested by fraudsters and immediately used to gain access to accounts and authenticate fraudulent transactions.

OTPs are often delivered to users via SMS, exacerbating the problem. With frequent attacks against GSM and 3G cellular networks, the confidentiality of text messages cannot be assured. On the device itself, trojans like Zeus, Zitmo, Citadel and Perkele leverage open access to SMS specifically to intercept OTPs. They have infected tens of millions of mobile devices worldwide, resulting in the theft of hundreds of millions of dollars. According to Kasperksy Labs, 2013 saw an almost twenty-fold increase in the number of recorded banking trojans, many of them targeting SMS OTPs.[19]

OTP: Security past its expiration date

For decades, the financial services industry has relied on OTPs for online banking security, but seismic shifts in computing power, the Internet and mobile technology and an explosion in digital crime have rendered these single-use strings of digits obsolete, both in terms of security and convenience.

For a comprehensive discussion of OTPs and their flaws, download Entersekt's white paper, *OTP: Security past its expiration date*.

Misplaced trust in this insecure channel has also opened banks and their customers up to mobile SIM swaps or SIM clones, number porting attacks, fake caller ID and call forwarding scams operated by dishonest customer service representatives at mobile carriers.

Ken Baylor does not mince his words in his analyst brief for NSS Labs: "Do not rely on SMS-based authentication; it has been thoroughly compromised."[20]

Solving the security and user experience equation

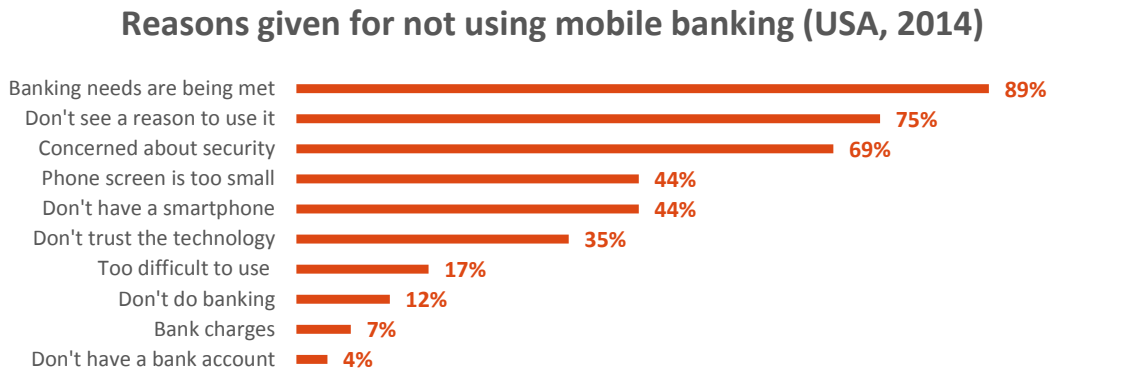
David Godsman is SVP Digital Banking, Emerging Payments and Innovation at Bank of America. When he was recently asked what the hardest part of his job was, he seemed not to miss a beat: "Meeting customer expectations – and I mean that in a sincere way," said the man tasked with keeping the bank's mobile offerings competitive. "Customers are experiencing digital environments in a variety of different fashions today. It is a very exciting time to be in banking, and it is a very intense time to be keeping pace with that, frankly."[21]

Mobile banking is evolving quickly. Users' heightened expectations of the channel have, to a degree, been driven by the sophistication of other online and mobile consumer services that they access – the near frictionless security measures, the intuitive design, the convenience of shopping online. "Why can't my bank be just a little bit more like Amazon?" they ask. People like David Godsman are working to answer them with a definitive, "It can be. It is."

X = security

As in the fledgling days of e-commerce when consumers were wary of providing their credit card details online, so today many banking customers doubt the security of mobile banking and payments. They are mindful of the wealth of personal information stored on their phones and suspicious of assurances that their data and money are adequately protected from mobile attack vectors.

The Federal Reserve Board's *Consumers and Mobile Financial Services 2014* report says that of US consumers who do not use mobile banking – a cohort still comfortably in the majority – 69 percent cited security as the primary reason for not doing so. Of those who do not make payments using their phones, 63 percent gave fears over the safety of the channel as the reason. Even early adopters of mobile banking often limit their activities to checking their account balances or recent transactions, shying away from money transfers or payments.[22]



Source: Board of Governors of the Federal Reserve System

To boost adoption and unlock the mobile's enormous potential, financial institutions must address their customers' security concerns by investing in new technology. Advertising and social media campaigns could then be used to highlight their efforts in this regard, strengthening the bonds of trust they share with their customers.

Y = usability

It seems ironic. As worried as they are about safety, consumers also report feeling frustrated by the security measures in place to protect them on this channel. Mobile functionality promises users casual, on-the-go convenience and instant accessibility like few technologies have ever done. On the other hand, small screen sizes and keypads, fluctuating download speeds, limited functionality and still immature user interface design can present hurdles that users of desktop computers need never worry about. Add to the mix obstructions that are intended to keep their accounts safe from intruders, and the entire experience can begin to feel onerous.

In a recent report from Deloitte, based on survey data from Andrews Research Associates, 24 percent of survey respondents said that the difficulty of seeing and typing on a smartphone was a "significant" factor limiting their use of mobile. Another 22 percent said it was a "somewhat significant" factor.[23] Forty-four percent of respondents in the Federal Reserve Board's mobile survey gave the small screen size of mobile phones as a main reason for not using mobile banking.[24] Older users may feature disproportionately among these respondents, but even so-called Millennials display an aversion for the keypad, signaling considerable interest in the use of mobile imaging and picture-based communication in mobile banking and payments.[25]

Mobile users want an easy to use, low-friction interaction, enabling them to execute transactions quickly, with a minimum of taps and key strokes, and little additional fuss. Whether

at a restaurant, on a train, or on the couch watching television, they don't want to type in OTPs or answers to challenge questions, or carry a second device, such as a hardware token.

For financial institutions to be successful in the era of mobile banking, it is important to design a secure mobile banking service that scores highly on user experience. "A poor mobile banking experience can be the single factor for a bank to lose a customer," according to Mike Stern, former director of business development at Xtreme Labs (since acquired by Pivotal). "It's surprising to see that there is a significant opportunity for top banks in the U.S. to improve their mobile offerings when it comes to user experience and application functionality."

Best practices to secure the mobile channel

Here are four steps banks can take to provide next-generation mobile banking security, build trust, improve usability and drive customer engagement.

Take full control of your security envelope

1. Avoid reliance on SMS, OTPs and native device security
2. Harness the power of public-key infrastructure on the mobile
3. Build a second, secure channel for user and transaction authentication
4. Take a layered approach to boost security for high-value, high-risk transactions

1. Avoid reliance on SMS, OTPs and native device security

Eliminate any technology that relies on OTPs, which are easily compromised; SMS message delivery, which is doubly vulnerable; and native mobile operating system device security, found time and again to be riddled with flaws. OTPs are a twentieth century solution; they cannot secure twenty-first century technology. They are also not an option for banks that sincerely care about designing apps for the unique way consumers engage with their mobile devices. That's true whether they are acting on a "mobile first" or simply a "human first" strategy.

2. Harness the power of public-key infrastructure on the mobile

Deploying industry-standard digital certificates to mobile phones and tablets allows them to be uniquely identified, transforming them into reliable second factors of authentication. Each certificate positively identifies a device, confirming a user's identity when logging onto the mobile banking app without them having to enter OTPs or answers to challenge questions, or rely on non-authoritative device fingerprinting techniques. Credit and debit card and call center interactions performed via the mobile device can also be authenticated in this way.

3. Build a second, secure channel for user and transaction authentication

End-to-end encryption of data substantially limits the chances of it being accessed or modified in transit. Any fraudster that does manage to do so could try to crack the encryption by brute force but this would take hundreds of thousands of years.

For truly secure user and transaction authentication on the mobile, banks should implement a separate, bi-directional channel between their servers and users' mobile devices. With the rapidly improving connectivity of mobile devices, whether on Wi-Fi, 3G or 4G networks, messages can be encrypted and sent to the device via push data messaging technologies, and the response encrypted and returned. This second, encrypted channel to the user can provide out-of-band, two-factor authentication on one device, without users even having to switch apps.

A second, encrypted channel to the user can provide out-of-band, two-factor authentication on one device, without users even having to switch apps.

Users receive real-time verification prompts and digitally sign approvals of all sensitive transactions with just one touch, reducing keystrokes, saving time and keeping them engaged. A Harris Interactive poll conducted for Entersekt in mid-2013 found 58 percent of US adults would be willing to take an active role in securing their online banking transactions if this meant using their mobile phones to authenticate activities.[26]

Properly securing the mobile channel in this way also allows banks to authenticate online banking logins and transactions, as well as card-not-present payments using the same interface, providing a consistent customer authentication experience across multiple channels.

4. Take a layered approach to boost security for high-value, high-risk transactions

Additional components or factors can be used to augment security for high-value transactions. These might include PINs, GPS location or other contextual data, and biometrics.

Biometrics is fast becoming a popular authentication method among mobile users as more devices come equipped with fingerprint readers. Deloitte reports that 72 percent of US consumers find biometric identification an appealing means of securing mobile for financial services.[27] It is an approach that can prove the owner of the device is currently in possession of it but not authenticate the customer per se. Combining this possession authentication with a PKI product such as Entersekt's Transakt, biometrics can be used to identify the user locally to a device, while a digital certificate is used to authenticate the user to the service provider. This is

the general approach followed by the FIDO Alliance, to which Google, PayPal, MasterCard, Visa, Bank of America and Entersekt belong.

Entersekt's authentication in your app

Entersekt helps banks eliminate online and mobile banking fraud while providing their customers with a truly distinctive, user-friendly experience. Our solution for mobile banking authentication secures the mobile banking app while eliminating the need for hardware tokens or OTPs.

Our software product, Transakt, lies at the center of all of our solutions. Available as a powerful SDK, Transakt uses industry-standard X.509 digital certificates and proprietary validation techniques developed specifically for the mobile channel to deliver the strongest possible device identification, obviating reliance on weak mobile device fingerprinting. Certificates can be combined with a PIN, password or fingerprint scan to identify the user and enable easy yet secure access to the app.

Transakt also creates a fully encrypted, out-of-band communications channel, based on mutual authentication, between the financial institution's servers and its customers' mobile devices. This channel means that the mobile device can constitute a true second factor of authentication even when performing mobile banking. For sensitive transactions real-time authentication requests can be sent out of band to the customer's mobile device. With just one touch, customers digital sign their "Accept/Reject" responses. There is no need to use a hardware token, enter lengthy OTPs, or even switch apps.

Entersekt's bottom line on biometrics

Large majorities of consumers in the developed world express interest in using their fingerprints to secure mobile banking and payments. This approach to authentication can improve their user experience by reducing manual input of information like passwords. As such, it will be particularly welcome to mobile users.

Entersekt supports fingerprint biometrics on Samsung and iPhone devices, but like many in the information security community, including the FIDO Alliance, we believe biometrics-based authentication should only be implemented as one part of a layered security system, especially in high-risk environments like digital banking.

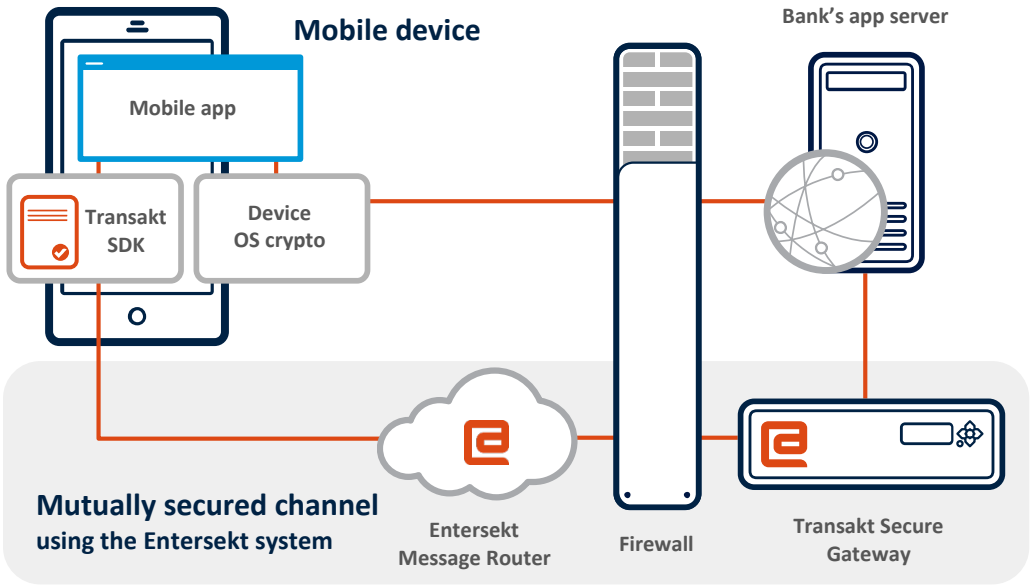
The FIDO-endorsed model for consumer biometrics requires users to self-enroll biometric information using their mobile device. Crucially, this data never leaves the phone. (This model is generally referred to as *private biometrics*. It addresses many of the privacy concerns and security risks that arise from the central storage of bulk biometric data by enterprises and governments. After all, the alternative is to surrender your irreplaceable biometrics data to organizations with a history of security breaches.) Since biometric data is not shared, its use is confined to proving that the user who input their biometric data on the device is currently operating it. This is not quite the same as proving who they are. "Biometrics as a convenient means of authentication are mass market, biometrics as a high security means of identification are not," says Dave Birch, director at Consult Hyperion, a global thought leader in digital identity and digital money. [28]

Deployed in conjunction with strong security – PKI, mutual digital certificates and encrypted messaging – fingerprints and other biometrics can be a significant additional tool in our efforts to deter account takeover activity with user-friendly, out-of-band authentication.

With this goal in mind, Entersekt supports biometrics to replace the input of user credentials and passwords, and to act as an additional data point. To guarantee that both the user and enterprise are legitimate and that their communications are as they intended, the device itself must be identified with a digital certificate, just as the enterprise is. In this way, the mobile device acts as a trusted second factor of authentication.

The financial institution retains full control over user registration, which is independent of networks or SIM cards. Deloitte has found that 80 percent of consumers want the ability to remotely disable a lost or stolen mobile device as a means of protecting their banking accounts.[29] With Transakt, the bank can revoke the digital certificate used to identify the device, immediately rendering the banking app unusable. Certificates are kept in a self-contained key store on the mobile device. This key store is off-limits to malware, because it is part of Transakt's sandbox, which no other application can access.

Entersekt's mobile banking authentication solution



The solution works with iOS, Android, BlackBerry, Windows Phone and feature phones capable of running Java applications, and requires no change in user behavior, and little or no user education.

To capitalize on the confidence they inspire in their customers, and to stay ahead of the fast-proliferating competition, it's vital that banks evolve their mobile offerings quickly, meeting customer demand for convenient functionality and a pleasant user experience while assertively addressing security threats. Entersekt helps you do just this: transform the mobile channel into a win-win for your institution and for your customers.

Further reading on entersekt.com

Solution sheet: *Mobile banking authentication*
[http://info.entersekt.com/mobile-banking-authentication-solution]

White paper: *The Importance of Transaction Signing to Banks*
[http://info.entersekt.com/the-importance-of-transaction-signing-to-banks]

White paper: *OTP: Security Past Its Expiration Date* (Second Edition)
[http://info.entersekt.com/otp-security-past-its-expiration-date]

Notes

[1] "Android Apps on Google Play"; AppBrain graph
[http://www.appbrain.com/stats/number-of-android-apps]
[2] "Number of available apps in the Apple App Store from July 2008 to September 2014"; Statista graph
[http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/]
[3] "Cumulative number of apps downloaded from the Apple App Store from June 2008 to October 2014 (in billions)"; Statista
[http://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/]
[4] *Consumers and Mobile Financial Services 2014* (March 2014); Board of Governors of the Federal Reserve System
[http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf]
[5] "Supplement to Authentication in an Internet Banking Environment" (June 2011); Federal Financial Institutions Examination Council
[http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf]
[6] "FFIEC may be prepping guidance for mobile banking" (July 26, 2013); Robin Arnfield; *Mobile Payments Today*
[http://www.mobilepaymentstoday.com/articles/ffiec-may-be-prepping-guidance-for-mobile-banking/]
[7] *BITS Mobile Technology – Layered Security Model* (June 2013); BITS/The Financial Services Roundtable
[http://www.bits.org/publications/doc/BITS_Mobile_LayeredSecurity_FINALJun2013.pdf]
[8] "*2014 Security Pressures Report*" (February 17, 2014); Trustwave
[http://www2.trustwave.com/rs/trustwave/images/2014%20Trustwave%20Security%20Pressures%20Report.pdf]
[9] "Study finds seven out of ten retail and finance applications vulnerable to Heartbleed-style attacks" (August 27, 2014); CAST press release
[http://www.businesswire.com/news/home/20140827005141/en/Study-finds-ten-retail-finance-applications-vulnerable]
[10] "Personal banking apps leak info through phone" (January 8, 2014); Ariel Sanchez; *IOActive Labs Research* blog
[http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html]
[11] "Weak Security in Most Mobile Banking Apps" (December 12, 2013); Kelly Jackson Higgins; *Dark Reading*
[http://www.darkreading.com/vulnerabilities---threats/weak-security-in-most-mobile-banking-apps/d/d-id/1141054]
[12] *View from the Precipice: Mobile Financial Malware* (December 11, 2013); Ken Baylor; NSS Labs
[https://www.nsslabs.com/sites/default/files/public-report/files/View%20From%20The%20Precipice%20-%20Mobile%20Financial%20Malware.pdf]
[13] *Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond* (December 9, 2013); Trend Micro
[http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf]
[14] "Mobile Malware Evolution: 2013" (February 24, 2014); *Securelist*, Kaspersky Lab
[http://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/]
[15] "FFIEC may be prepping guidance for mobile banking" (July 26, 2013); Robin Arnfield; *Mobile Payments Today*
[http://www.mobilepaymentstoday.com/articles/ffiec-may-be-prepping-guidance-for-mobile-banking/]
[16] "Introducing nogotofail—a network traffic security testing tool" (November 4, 2014); Chad Brubaker; *Online Security Blog*, Google
[http://googleonlinesecurity.blogspot.ro/2014/11/introducing-nogotofaila-network-traffic.html]
[17] "The most dangerous code in the world: validating SSL certificates in non-browser software"; M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, V. Shmatikov; *ACM Conference on Computer and Communications Security*, October 16–18, 2012
[http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf]
[18] *Secure M-Commerce Through Three Categories of Mobile User Authentication and Fraud Prevention* (September 20, 2013); Avivah Litan, John Girard; Gartner research note
[19] "Mobile Malware Evolution: 2013" (February 24, 2014); *Securelist*, Kaspersky Lab
[http://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/]
[20] *View from the Precipice: Mobile Financial Malware* (December 11, 2013); Ken Baylor; NSS Labs
[https://www.nsslabs.com/sites/default/files/public-report/files/View%20From%20The%20Precipice%20-%20Mobile%20Financial%20Malware.pdf]
[21] "Q&A: At Bank of America, mobile strategy evolves in competitive space" (October 14, 2014); Deon Roberts; *The Charlotte Observer*
[http://www.thestate.com/2014/10/14/3743888_qa-at-bank-of-america-mobile-strategy.html]
[22] *Consumers and Mobile Financial Services 2014* (March 2014); Board of Governors of the Federal Reserve System
[http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf]

[23] "Mobile financial services: Raising the bar on customer engagement" (May 19, 2014); Val Srinivas, Sam Friedman, Jim Eckenrode; Deloitte Center for Financial Services [http://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/05/DUP-693_FSI-Mobility_MASTER_kw.pdf]
[24] *Consumers and Mobile Financial Services 2014* (March 2014); Board of Governors of the Federal Reserve System [http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf]
[25] "Smartphones Changing the Way Millennials Bank" (September 25, 2014); Ann Reichert; *The Financial Brand* [http://thefinancialbrand.com/42513/mobile-banking-millennials-photo-research/]
[26] "Entersekt Poll: Banks Risk Shattering Customer Trust with Lax Stance on Fraud" (August 22, 2013); Entersekt press release [http://www.businesswire.com/news/home/20130822005136/en/Entersekt-Poll-Banks-Risk-Shattering-Customer-Trust]
[27] "Mobile financial services: Raising the bar on customer engagement" (May 19, 2014); Val Srinivas, Sam Friedman, Jim Eckenrode; Deloitte Center for Financial Services [http://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/05/DUP-693_FSI-Mobility_MASTER_kw.pdf]
[28] "Mobile phones and biometrics are a winning combination in the mass market" (June 17, 2014); Mobey Forum blog [http://www.mobeyforum.org/mobile-phones-and-biometrics-are-a-winning-combination-in-the-mass-market/]
[29] "Mobile financial services: Raising the bar on customer engagement" (May 19, 2014); Val Srinivas, Sam Friedman, Jim Eckenrode; Deloitte Center for Financial Services [http://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2014/05/DUP-693_FSI-Mobility_MASTER_kw.pdf]

Important notice

Entersekt, Tower Place 100, Suite 620, 3340 Peachtree Road NE, Atlanta GA 30326, USA

Phone: +1 404 698 1001

Email: info@entersekt.com

Web: www.entersekt.com

Document ID: ENTERSEKT-40-1038