Safe Mobile Apps for Financial Services

Who should read this paper

Financial services institutions that want to understand how Symantec protects mobile services from exploits with easy-to-use, transparent two-factor authentication within your branded solutions.

Advice offered about:

- Understanding the need for robust mobile security
- Identifying benefits and challenges of deploying two-factor authentication
- Using Symantec's cloud-based VIP Service to quickly protect your mobile services
Content

Executive Summary ................................................................. 1
Now Is the Time to Boost Mobile Security ................................ 1
Traditional Two-Factor Authentication is Hard to Deploy and Use .................................................. 2
VIP: Stronger Mobile Security, Simpler to Use ................................................................. 3
  Symantec VIP Service Features ................................................................. 3
  How the VIP Service Works ................................................................. 4
Mobile Banking Case Study ................................................................. 5
Symantec Code Signing for Mobile - Best Practices in Action ......................................................... 5
Learn More ................................................................................................. 6
Executive Summary

For financial services companies, the global surge in smartphones has set the stage for broader consumer use of mobile financial services. According to new data from Google, more than 50 percent of the population has smartphones in Australia, UK, Sweden, Norway, Saudi Arabia, and the UAE. More than 40 percent penetration now exists in the United States, New Zealand, Denmark, Ireland, Netherlands, Spain, and Switzerland. Google notes, "Mobile devices have become indispensable to people's lives and are driving massive changes in consumer behavior." Among these are users who have begun to embrace mobile financial services. In the U.S., nearly half (48 percent) say they want to compare prices while shopping. About a third desire to receive location-based offers and promotions, track finances, and manage discount offers with their smartphone, according to research by the Federal Reserve.

However, as for mobile financial transactions, usage is lower. For example, Federal Reserve data notes that just 21 percent of mobile phone owners have used mobile banking during the past year. Of those, 90 percent simply check account balances or recent transactions, and 42 percent transfer money between accounts. Only 12 percent of mobile phone owners have made a mobile payment during the last 12 months. According to the Federal Reserve, the main reason impeding mobile payments and banking is people are concerned about security of the technology. The same fear of insecurity was confirmed by Google’s study. Other reasons cited were “too complicated,” “payment features not available,” and “payment too complex.”

Financial institutions have high hopes for mobile. Goals include differentiating their services, improving customer “stickiness,” cutting costs with automation, and attracting the “unbanked” into their electronic fold. But to reach these objectives, financial services providers must first address the issue of mobile security. Mobile customers must feel secure in using those services – otherwise, the services will face ongoing customer resistance. This paper describes a simple, cost-efficient way to add robust security to managed and unmanaged mobile devices.

By using two-factor authentication with Symantec™ Validation and ID Protection (VIP) cloud-based service, financial services companies can quickly secure access to mobile financial services and data – all with an easy-to-use, transparent authentication interface presented as part of your branded mobile solutions.

Now Is the Time to Boost Mobile Security

Part of consumers’ fear about mobile security is unfamiliarity with the devices and how they are protected from attacks. The Google study says 65 percent of respondents prefer a PC or laptop to conduct ecommerce. Many consumers are familiar with using security controls on those devices such as antivirus, anti-malware, firewall, intrusion detection and prevention, and updating operating system and application software. Security for mobile transactions is more obscure, so they feel safer using PCs for online transactions.

Consumers are right to be concerned with security on mobile devices. While the number of immediate threats to mobile devices remains relatively low in comparison to threats targeting PCs, there is a significant number of emerging vulnerabilities affecting mobile devices. In a

1- Google, Our Mobile Planet, May 2012 at http://www.ourmobileplanet.com
4- European Retail Banking eBusiness And Channel Strategy, Forrester Research, Inc., April 25, 2012
recent report by Symantec’s global security research team, Symantec documented 315 vulnerabilities in mobile device operating systems in 2011 compared to 163 in 2010 – an increase of 93 percent. The top three categories of mobile vulnerabilities focused on the compromise of SMS, which can result in compromise of the devices, including the use of credentials for accessing sensitive applications such as online shopping and banking. Traditional endpoint exploits such as modification of configuration settings, manipulation of application privileges, and injection of Trojan applications occurred with less frequency on mobile devices. We expect the frequency of exploits like these will rise on unprotected devices as criminals gain more experience with mobile devices and applications. A detailed analysis of mobile threats is presented in the report.

As with traditional endpoints, securing managed and unmanaged mobile devices and applications entails the use of multiple layers of security controls. These require the joint cooperation of mobile application developers, wireless network service providers, and IT experts in the financial institution. The single most effective control to thwart mobile exploits is two-factor authentication (2FA). It enhances traditional account access security by requiring two or more of the three authentication factors: something a user knows such as a password or PIN, something a user has such as a smart card or hardware token, and something a user is such as a fingerprint or eye retina pattern. Multi-factor authentication is widely accepted as a strong security control. It is specified as a minimum control expectation by the U.S. Federal Financial Institutions Examination Council, and as an effective technique to authenticate customers for high-risk transactions. Two-factor authentication is prescribed by the PCI Security Standards Council to secure remote-access solutions transmitting cardholder data.

Traditional Two-Factor Authentication is Hard to Deploy and Use

The steps to secure mobile financial transactions can be complex and challenging. Required layers include security of the mobile device, the application running on the device, authentication of the device connecting to a service provider, account access security, and encryption of sensitive data - both stored and transmitted. Our focus here is two-factor authentication and for true 2FA, the second factor usually is something a user has, such as a hardware token or USB plug.

Usually these tokens are proprietary and are each assessed an annual user fee of $50 to $100. This cost becomes prohibitive with hundreds of thousands or millions of retail customers. Even if cost was no object, physical tokens are easily lost, which thwarts consumers’ ability to logon and use the mobile financial service. Deployment is challenging and an organization must devote resources to manage lost, damaged, or reissued tokens. Support costs can quickly escalate, especially for end users who struggle with installation of a client-side software certificate or responding to 2FA processes. When 2FA is complicated, users often give up and will not use the mobile solution. On the back end, organizations that operate 2FA internally must commit capital expenditures and operational expenditures for deployment and ongoing operations. Finally, execution of 2FA is time sensitive, so internally-run 2FA requires an IT architecture and components that meet strict performance SLAs.

For these reasons, traditional 2FA solutions have yet to achieve widespread adoption for large-scale consumer financial solutions. Financial institutions that want to competitively differentiate with mobile solutions need a better way to boost mobile security with 2FA.

Symantec is a leading provider of strong authentication

- 15 million VIP credentials currently under management
- 220 million device certificates
- 12 million credential downloads / month
- 15 million certificates issued from processing centers

VIP: Stronger Mobile Security, Simpler to Use

Symantec Validation and ID Protection Service (VIP) is a leading cloud-based strong authentication service that enables consumers to securely access mobile solutions. It provides peace of mind to consumers by adding strong security for mobile services. VIP’s cloud-based architecture reduces costs and complexity, allowing organizations to quickly and easily deploy strong authentication without up-front capital expenditures. It provides flexible authentication options and allows a mobile phone to serve as the second credential for 2FA. Consumers may misplace hardware tokens, but 80 percent of smartphone users never leave home without their phones in hand, according to the Google study. Symantec VIP includes a highly customizable SDK that supports a wide variety of mobile devices with your current workflows, and transparently integrates 2FA with your solution brand.

VIP is designed and operated for strong security:

- 15-year track record protecting critical infrastructure
- Hardware security module-generated keys and AES-encrypted storage
- Physical Security – cloud operations housed in Tier 4 data center physically and logically separated from Symantec’s corporate network
- Certifications & Compliance – PCI DSS, SAS-70 Type II, WebTrust for Certificate Authority and federal government PKI
- Service management governed by strict control processes
- Systems and Security Monitoring – Dedicated 24x7 network operations center, global monitoring, daily vulnerability scans, and many other security controls

Symantec VIP Service Features

- Cloud-based infrastructure – Secure, reliable, and scalable service delivers authentication without requiring dedicated in-premise server hardware.
- Multiple two-factor credential options – Deploy one-time-password credentials in a variety of hardware, software, or mobile form factors.
- Free mobile device credentials – Support for more than 850 mobile devices including Android™, iOS, Windows™ Phone 7, and J2ME.
- Transparent risk-based authentication – Leverage device and behavior profiling to block risky logon attempts without changing the user’s logon experience.
- Out-of-band authentication support – Authenticate users via SMS messages or voice-enabled phone calls when elevated risk is detected.
- Transaction monitoring support – Evaluate activity related to end-user’s monetary transactions, including anomalous amount, anomalous destination, transaction velocity anomaly, and high risk touch points, which allows the organization to challenge the user with an additional factor of authentication.
- Enterprise infrastructure support – Also integrates with popular enterprise VPNs and corporate directories to support internal mobile applications.
- Self-service credential provisioning – Deploy strong authentication to consumers without requiring IT helpdesk or administrator configuration or intervention.
- Web-based application integration – Add strong authentication to your application using the Symantec VIP web services API in your preferred programming language.
How the VIP Service Works

VIP also ensures the user’s logon request is originating from a known, registered device. Its risk-based authentication feature examines characteristics of the user’s endpoint device and logon behavior to assess the likelihood that the logon request originates from a legitimate user. In essence, VIP allows the user’s device to act as the “something you have,” and the user’s behavior to provide the “something you are.” VIP defends your organization against high-risk logon attempts from malicious sources identified by the Symantec™ Global Intelligence Network, a global network providing comprehensive, up-to-date information on sources of malicious Internet activity.

VIP provides additional protection for mobile services by analyzing and providing risk analysis information for each user transaction. If the transaction is anomalous or suspicious compared to past user behavior, the risk score is higher, allowing financial institutions to challenge the user for additional authentication. VIP also monitors monetary transfer amounts for unusually large transfers, new or unknown destinations, unusual transaction velocity, and high risk activity such as monetary transfer requests made at the same time as changes to account details.
Workflow Steps for Smartphone-based 2FA with VIP

1. **User requests access.** “PIN and IN” technology leverages the one-time password (OTP) as a dynamic device ID for quick logon. Simple deployment and activation. Deploys extra layer of security to bolster user confidence. User enters a username and password, or only a PIN to access a mobile application.

2. **Phone requests access.** Via an invisible OTP, the phone requests access to the organization’s back-end VIP application server.

3. **Organization’s VIP server allows access.** Integration with the back-end VIP application server is made with a few calls via our SOAP web services API. The same API can also integrate VIP multi-factor authentication for regular web applications.

4. **VIP service validates OTP.** The backend VIP application server validates the OTP via the VIP cloud-based service. Validation can include other API-controlled processes such as checking with the Global Intelligence Network to evaluate characteristics of a particular logon request. Upon validation, the user is granted access to the mobile application.

Mobile Banking Case Study

**Who:** A US bank operating globally with 23,000 employees, serving eight million customers.

**Business Need:** The bank wanted to offer mobile banking services via an Apple iPhone client. It sought to include strong authentication without compromising the user experience, meet FFIEC guidance, enable easy global deployment, and be cost efficient to deploy and manage. Early adoption of an initial solution was poor because the authentication process required too many steps (for example, manual entry of a user name, password, and PIN).

**Solution:** The bank chose to deploy Symantec VIP using a “silent second factor” for a quick, transparent logon experience.

**Results:** Without any promotion, 40,000 customers began using the mobile application within three weeks; almost half a million customers used the app within a year. More than 70 percent gave a 5-star rating in the iTunes Store along with excellent comments for the Quick Logon feature. Most of these customers are using the mobile app as their primary way to access the bank’s services.

Symantec Code Signing for Mobile - Best Practices in Action

In this paper, we’ve focused on the service provider’s perspective for strengthening authentication to mobile financial services that are accessed primarily with unmanaged consumer devices. As noted, consumers are concerned about the general security of your mobile financial services. Symantec helps financial services companies to prove their mobile services are legitimate and trustworthy with digital signatures. These act as a digital shrink wrap to demonstrate integrity of mobile applications that cannot be altered and distributed with unapproved changes. Symantec provides digital signature, authentication, and private key management solutions for mobile application developers and distributors, facilitating the verification of a publisher’s identity and confirmation of the trustworthiness of an application.

Our code signing services support every major desktop and mobile software platform, including devices running both Android and Windows Mobile. Symantec offers the only dedicated root certificate for the Android platform and has a full signing and key management service for Android developers. Symantec is also the exclusive code signing certificate provider for all Windows Mobile application development.

Five Best Practices

- Employ Device ID analytics: non-cookie based strong authentication cannot be easily compromised
- Utilize threat intelligence data such as that collected by the Global Intelligence Network to stay ahead of emerging threats
- Integrate with endpoint solutions such as Norton or Symantec Endpoint Protect to review the health and reputation of a device before it gains access to your network
- Configure out-of-band challenges for risk-based anomalies or suspicious behavior to mitigate man-in-the-middle attacks
- Implement behavior analysis to enable self-learning anomaly detection
All Symantec code signing customers go through a rigorous authentication process. Signing your mobile application with a Symantec certificate shows that you are trusted by the leader in code signing security and helps ensure a safe, secure experience for you and your customers. Re-creating a self-signing architecture would be cost-prohibitive and places an organization at much greater risk for security breaches.

For more information on Symantec Code Signing for Mobile, please visit go.symantec.com/code-signing. You can also access TCO-focused information using SSL intranet certificates at this address: https://forms.verisign.com/websurveys/servlet/ActionMultiplexer?Action_ID=ACT2000&WSD_mode=3&WSD_surveyInfoID=1703&toc=7DWGF-1703-01-26&brand=01&country=26&cid=D073BAA39DF5F5F2

Learn More

Financial services organizations have an opportunity to leverage the vast adoption of smartphones with mobile financial services. The catalyst is fostering customer trust in the security of mobile solutions. With Symantec VIP, your organization can quickly secure those solutions with strong 2FA. With its cloud-based infrastructure, VIP can rapidly scale to large consumer-application requirements for mobile solutions deployed under your own brand. For more information about protecting mobile solutions or Symantec VIP, contact your Symantec representative or visit our website at www.symantec.com/verisign/vip-authentication-service.
About Symantec

Symantec protects the world’s information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.