

November 16, 2007

Mobile Authentication Marries Security With Convenience

by Bill Nagel

for Security & Risk Professionals



November 16, 2007

Mobile Authentication Marries Security With Convenience

A Token-Killing Form Factor For Secure Consumer Online Banking

by **Bill Nagel**

with Thomas Raschke, Jonathan Penn, and Onica King

EXECUTIVE SUMMARY

Financial institutions seeking to expand their online and mobile banking offerings to their entire customer base face the age-old challenge of balancing security with usability. Many banks feel trapped: Fail to implement strong authentication and incur the wrath of auditors, or roll it out and risk losing customers that find it too inconvenient to use. These banks often compromise on a method that ticks the boxes on audit sheets but fails to deliver strong security. But several vendors now leverage the near ubiquity of mobile phones to provide a range of secure, effective, and convenient methods of customer authentication. Mobile authentication can be the linchpin that holds together online banking, mobile banking, and mobile payments in a way that marries security with convenience — increasing the chances that banks will heed the advice of their security professionals. To sell all sides on the value of mobile authentication, look for solutions that offer several levels of convenience to make customers happy on the front end and a flexible, modular architecture to ease management on the back end.

TABLE OF CONTENTS

2 Banks Are Recognizing the Value Of Greater Online Security

3 Mobile Authentication Takes Advantage Of The Token You Already Have

Delivering OTPs Via SMS Allows Late Adopters To Embrace The Familiar

Generating An OTP Via A Soft Token Offers Flexibility To The More Ambitious

Out-Of-Band Authentication Reassures The Security-Savvy With Maximum Protection

RECOMMENDATIONS

9 Adopt Flexible, Multifunctional Solutions With Customers In Mind

10 Maximize The Mobile Channel's Security Value: Authenticate The Transaction

WHAT IT MEANS

11 More Convenient Authentication Factors Will Supplant Traditional Tokens

11 Supplemental Material

NOTES & RESOURCES

For this report, Forrester interviewed banks, systems integrators, and vendor companies including Authentify, ClairMail, Deepnet Security, Diversinet, Fronde Anywhere, Gemalto, RSA Security, Secure Computing, StrikeForce, Valimo Wireless, and VASCO.

Related Research Documents

["Online Banking Holdouts Still Want Security Guarantees"](#)

June 21, 2007

["Function-Rich Mobile Finance In Europe: Not Ready For Prime Time In Retail Banking"](#)

June 21, 2006

["VeriSign Goes VIP"](#)

April 7, 2006

["Online Banking Security: Give Customers More Control And Reassurance"](#)

January 4, 2006

BANKS ARE RECOGNIZING THE VALUE OF GREATER ONLINE SECURITY

Online security today requires more than just usernames and passwords for user authentication — and the need is particularly critical in financial services.¹ As strategies for phishing and other forms of online fraud grow more sophisticated, adopting stronger authentication methods is becoming a matter of protecting the bottom line for banks, other financial institutions, and eCommerce sites. Stronger authentication has been a way of life for years in some geographies, but others — even technologically advanced ones — have been slower to jump on the bandwagon. For example, many banks in Europe, particularly in the Benelux and Nordic countries, long ago implemented effective multifactor authentication (MFA) for all of their online banking customers, including retail banking. Customers had no choice in the matter: The banks mandated the system, whether for regulatory reasons or to prevent fraud loss; security and antifraud took precedence, and the end user just had to deal with it.

However, this has not proved as suitable in less regulated markets like the UK and US, where banks are more concerned about churn in their retail customer base and are thus less willing to pioneer strong authentication.² Financial institutions seeking to implement MFA have historically been able to choose from a number of different methods and form factors, including one-time password (OTP) tokens, OTP challenge/response calculators, smart cards with readers, numeric grids printed on cards or sheets of paper, and various combinations of the above.³ While most banks across the globe have implemented strong authentication for their commercial customers, many in the US and UK have shied away from doing so on the consumer side, considering it:

- **Too costly for the institutions.** OTP tokens and OTP-generating calculators from the likes of ActivIdentity, Aladdin, Entrust, RSA Security, and VASCO cost anywhere from \$5 to \$40 per unit, depending on functionality; they typically have a three-year replacement cycle. Smart cards are generally cheaper — \$2 to \$10 — and, as with chip and PIN cards, often already baked into the cost of doing business. But plastic cards are easier to lose, wear out more quickly, and require a reader for OTP generation — which tacks on another \$8 to \$15 per unit. Combine this with distribution and user education costs, and it's no surprise banks balk.
- **Too complicated to deploy and manage on a mass scale.** It's not just the cost of buying, distributing, and replacing tokens that causes pain — it's the logistics of doing so. It's the same problem as managing the distribution and replacement of ATM cards and PINs, which is familiar enough; but as ATM cards and PINs aren't going away anytime soon, adding token distribution to the mix is not a particularly attractive prospect.⁴
- **Too inconvenient for consumers.** MFA requires people to use something other than “what they know” — passwords, out-of-wallet questions — to perform online banking functions. Business banking customers, professionally used to dealing with the risk of losing large sums, take easily to MFA. But while retail customers clearly want their accounts to be secure, they're also much more willing to sacrifice security for convenience if they perceive that higher-security options require too much of them.⁵ Many consumers, especially those with multiple accounts or a need to access

their accounts from multiple or remote locations, find none of the traditional MFA options particularly attractive, as most of them require carrying a separate device to access each account or effectively tie account access to a single computer.⁶ The prospect of carrying around — and possibly losing — a pocketful of OTP tokens, a walletful of cards, or some card readers is one many consumers aren't willing to face.

MOBILE AUTHENTICATION TAKES ADVANTAGE OF THE TOKEN YOU ALREADY HAVE

The promise of strong authentication using a mobile phone attracts institutions already employing two-factor authentication (2FA), as well as many others that are considering it but worry about cost and convenience. A number of vendors have taken an approach that leverages the near ubiquity of mobile phones in many markets. These vendors have developed solutions that send OTPs to customers' mobiles, generate OTPs directly on those mobiles, or use the phone as a separate authentication channel. Several solutions do more than one of these — and offer an authentication architecture that also supports traditional MFA methods.⁷ Mobile authentication helps banks overcome consumer reluctance by offering them a range of convenient, secure options while saving rollout and ongoing administration costs.

Vendors offering mobile authentication solutions take advantage of several different mobile phone capabilities: sending and receiving text messages (SMSes); downloading and running Java applications; browsing the Internet over the air or via Wi-Fi; and containing a programmable smart card (SIM card) that can hold additional identity credentials. And it's a two-way channel — either the customer or the bank can initiate the interaction. The available solutions balance security, convenience, and cost in different ways.

Delivering OTPs Via SMS Allows Late Adopters To Embrace The Familiar

The most basic mobile authentication option, and the one most likely to appeal to late adopters, is delivering an OTP via SMS (see Figure 1). An online banking customer logging in to the bank's Web site with his username and password triggers a request to send an OTP to his registered mobile phone. When the customer receives the text message, he enters the OTP contained therein into an additional field on the banking site's login page, using this second factor to complete the login process. Banks that require customers to additionally authenticate certain transactions can also use OTP SMSes for this purpose.

SMS OTP delivery is simple and familiar. Most handsets can receive texts — it's one of the most basic tasks on a mobile.⁸ The method only requires the customer to register a mobile number with the bank and notify it if the number changes. The login process is as straightforward as when using any other form of OTP hardware token; there's no need to actually keep track of extra hardware — just wait for the text message to arrive. This factor certainly appealed to Citibank customers in Singapore: When offered the option of receiving OTPs via text message or by using a hardware token, 80% of them opted for SMS. However, this simplicity is not without its drawbacks, in that this option:

- **Pushes extra costs onto some end users.** Some mobile customers, particularly in North America, have to pay for the SMSes they receive — adding per-use costs to this method of mobile authentication. End users unlucky enough to pay to receive SMSes and who bank with an institution that requires authentication via OTP to set up new payees or confirm transactions could balk at the costs associated with this form of online banking. Most don't, though: \$0.03 to \$0.15 per received SMS has not proved unduly onerous.⁹ A major New Zealand bank was bold enough to tack on a \$0.19 bank-side fee for each SMS delivery — and still attracted 35,000 customers to the service in the first 10 months after introduction.
- **Is subject to network coverage, network latency, and SMS delivery issues.** One hitch to receiving OTPs via SMS is making sure that the text actually reaches the recipient. Mobile carriers don't guarantee that SMSes will be delivered quickly — or at all; customers trying to do their banking in areas with poor or nonexistent network coverage can find themselves out of luck.¹⁰ About half of the banks we spoke with don't view this as a big enough issue to delay rolling out SMS-based mobile authentication; the rest are more conservative. In any case, SMS OTP is the entry-level, lowest-common-denominator version of mobile authentication.
- **Doesn't address the man-in-the-middle problem.** As with the more traditional key-fob form of OTP tokens, SMS OTPs are susceptible to man-in-the-middle attacks — as ABN AMRO in the Netherlands found out the hard way.¹¹ If the user is actually visiting a phishing site or a keylogging program has been covertly installed, then the session is still vulnerable to a fraudster sitting between the client computer and the bank computer. OTPs make it more difficult for fraudsters, but not impossible for the sufficiently determined.

Figure 1 SMS Is The Most Basic Way To Deliver An OTP



42982

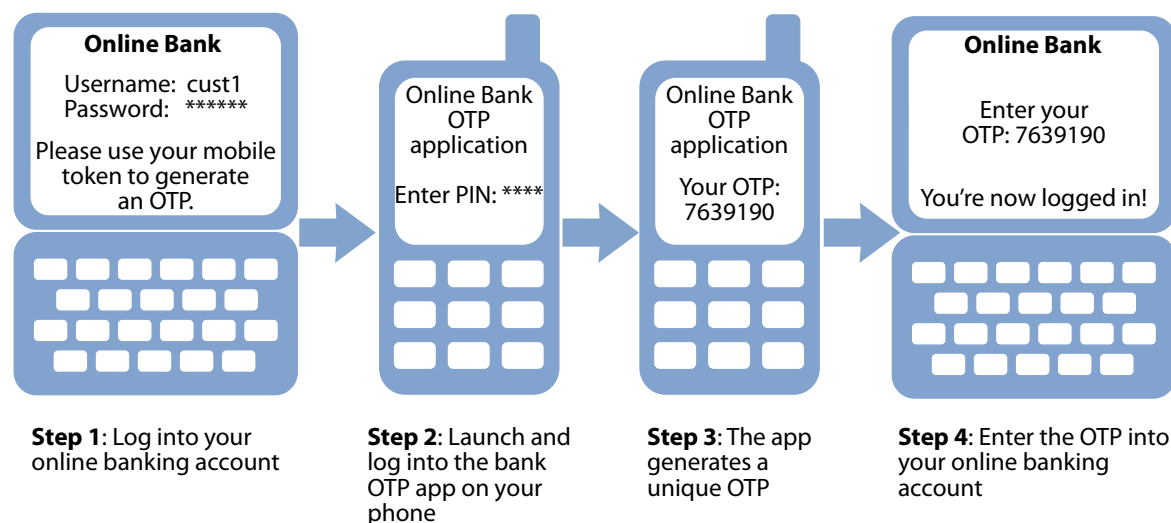
Source: Forrester Research, Inc.

Generating An OTP Via A Soft Token Offers Flexibility To The More Ambitious

The next step up the mobile authentication ladder is to turn the mobile phone into a “soft token” by installing software that generates OTPs on the phone itself. The most common OTP generators are for Java-enabled phones, including BlackBerry, Palm OS, Symbian, and Windows Mobile for Pocket PCs and/or smartphones; some of them issue time-based OTPs and others issue event-based OTPs. A few vendors, like Gemalto and VASCO, provision the OTP application on a SIM card rather than having the end user download it into phone memory. Valimo Wireless puts a digital signing app on SIM cards that can authenticate logins, sign transactions, and more. This approach, while slightly more complicated than SMS from a rollout and support standpoint, offers advantages in terms of cost and usability. The advantages of the soft token approach are that it:

- **Is simple to use — once the software’s installed.** As far as the customer is concerned, this method works in essentially the same way as SMS OTPs, except that instead of waiting to receive an automatically generated SMS, the user runs the OTP app on his phone, requests an OTP, and receives it instantly (see Figure 2). Customers wishing to use this method need to have a Java-enabled phone — the bulk of the phones sold in the past three years. Banks need to anticipate requests for help with software installation and time synchronization.
- **Incurs no extra costs aside from the software download.** As the user does not use any airtime or carrier services to generate the OTP, this method doesn’t cost users anything. Depending on the carrier and download method, customers may have to pay to download the app. And unlike SMS delivery, which only cares about the number on the SIM card and not which handset the SIM card is in, customers who get a new mobile will need to download and install the app again — unless the soft token solution of choice uses an app residing on the SIM card itself.

Figure 2 An OTP-Generating Soft Token On A Mobile Is Flexible And Works Off The Mobile Network



42982

Source: Forrester Research, Inc.

- **Is immune to coverage, latency, and delivery issues.** Doing everything on the phone itself very nearly completely immunizes users from the vagaries of mobile networks — making the soft token approach a better choice for mobile payments.¹² But one issue remains with certain soft token solutions: time synchronization. If the product uses time-based authentication, but the handset does not support Greenwich Mean Time or synchronizes incorrectly when crossing time zone borders, the OTP generator on the phone will be out of sync with the authentication server; the phone will generate “incorrect” OTPs and the user must intervene manually.

Soft tokens are no panacea, though; in practice, they provide neither complete coverage nor complete protection. Specifically, soft tokens:

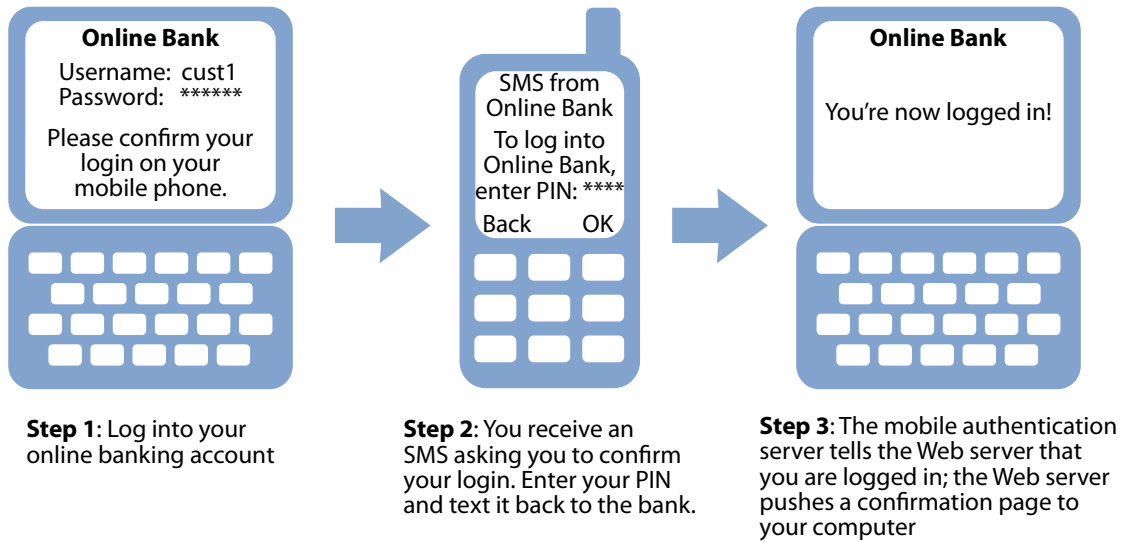
- **May require customers to get new service contracts.** Users need to have data services in their mobile subscription to be able to download a soft token app to their handsets. And the number of consumers with data subscriptions is but a fraction of those with text messaging capabilities. For example, 78% of European and 35% of North American mobile users send and receive SMSes, but in each case just over 10% use the mobile Internet.¹³ While not all data-capable subscribers use the service for browsing or downloading from the Internet, this indicates that the user base for soft tokens is primarily the early adopter community.
- **May require customers to upgrade their devices.** The majority of handsets produced in the past three years can run Java applications, and over 700 million mobile phones worldwide are Java-enabled.¹⁴ Still, many brand-new, popular handsets — including Apple’s iPhone — don’t support Java. To expand soft token uptake beyond the roughly half of current subscribers with a Java-enabled phone, banks will need to rely on consumers upgrading their mobiles — a behavior that is inconsistent at best. And just because a handset is “Java-enabled” doesn’t guarantee compatibility.¹⁵
- **Don’t address the man-in-the-middle problem.** As with OTP delivery via SMS, the soft token method does not execute the second factor over a separate channel, so a customer using a compromised computer can still fall victim to a determined attacker.

Out-Of-Band Authentication Reassures The Security-Savvy With Maximum Protection

There is a way to thwart the possibility of a man-in-the-middle attack: perform the second authentication factor over a channel completely separate from the Internet; authenticate the transaction as well as the login; and provide transaction details to the customer as part of the transaction authentication. This is where the use of the mobile phone for MFA really shines, and security-oriented customers are likely to embrace this option. Including transaction authentication is the key here; receiving and confirming a PIN via a handset is, from a security standpoint, equivalent to receiving a PIN on the device and then entering it into the Web session. But the ability to receive transaction details on the mobile — whether by voice or SMS — and confirm the transaction via a completely separate channel eliminates the man in the middle. The out-of-band (OOB) approach:

- **Is not difficult to use — but may require educational outreach.** Most of the OOB approaches on the market are not difficult to use; however, OOB is still a bit less intuitive. In theory, it's easy, although a less familiar concept than “get an OTP and enter it into the bank's Web site alongside my username and password” (see Figure 3). As such, banks should take greater care to develop effective user documentation and other educational materials than they do when implementing other MFA systems. The upside: Early adopters will be the ones most likely to grasp the concept — giving banks some leeway to work out the kinks before pushing it out to a broader audience. The downside: The fraction of online banking consumers security-savvy enough to embrace OOB within a timeframe relevant to bank ROI may be too small for some banks to take the plunge.
- **Usually pushes no extra costs on the user.** In most cases, the authentication system calls or texts the user, not the other way around — so only those customers who pay to receive calls will get hit with extra costs. As with OTP via SMS, customers who pay to receive texts — or whose bank has implemented an OOB system that requires the user to text the bank back — will also incur per-session or per-transaction costs. But security-savvy customers — the initial adopters of OOB authentication — are even less prone to balking at paying a small premium for really secure online banking than SMS OTP adopters.
- **Is susceptible to coverage, latency, and delivery issues.** Because OOB authentication has to occur in real time over the mobile channel, several possible issues arise: network coverage, for both SMS delivery and voice calls; voice quality problems; and SMS latency and nonguaranteed delivery. This makes the choice of OOB authentication highly dependent on the quality of mobile phone service in a given country or region.
- **Foils the man in the middle when used with transaction authentication.** Mobile authentication that confirms the transaction details and performs the second authentication factor for the transaction over a separate channel is one of the few methods that solve the man-in-the-middle problem for a reasonable price — both in terms of flexibility and ease of use and of actual cost (see Figure 4). Out-of-band transaction authentication offers the additional benefit of mutual authentication: The bank is certain that it's carrying out legitimate customer intentions, and the customer knows that the bank will only perform the transactions she wants to make — rather than those of a fraudster sitting in the middle of her online banking session.

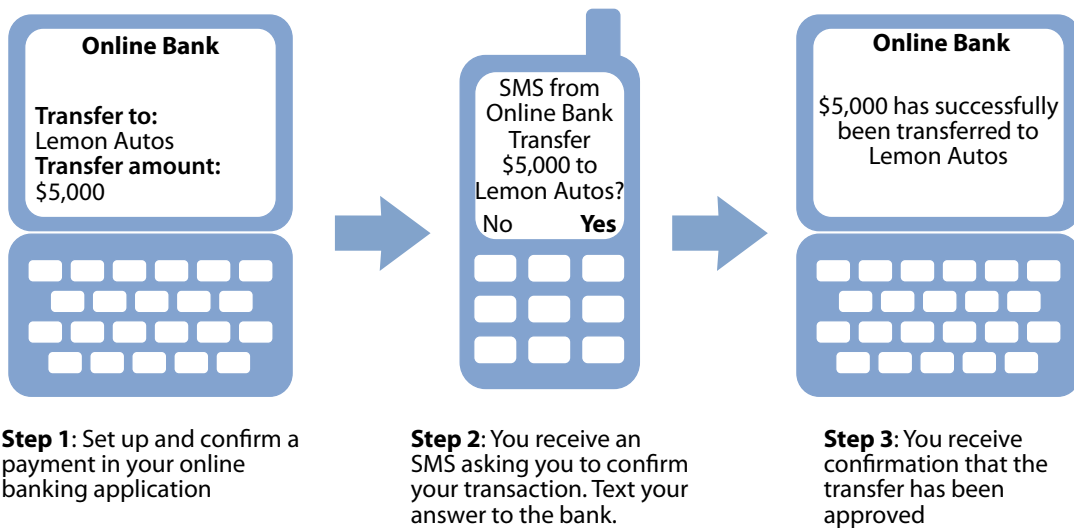
Figure 3 Mobile Can Provide A Convenient, Separate Login Channel



42982

Source: Forrester Research, Inc.

Figure 4 Over-The-Air Challenge/Response Enables Simple, Secure Transaction Authentication



42982

Source: Forrester Research, Inc.

RECOMMENDATIONS

ADOPT FLEXIBLE, MULTIFUNCTIONAL SOLUTIONS WITH CUSTOMERS IN MIND

Mobile authentication helps security pros make the business case for implementing proper multifactor authentication for all banking customers. Adopting mobile authentication accomplishes several primary goals for banks: improving the security of existing online and mobile banking customers; bringing more retail banking customers, including late technology adopters and token skeptics, into the strong authentication fold through increased consumer choice and ease of use; lowering the risk of transaction fraud; and reducing or eliminating token rollout and support costs. Retail customers will adapt, and banks that proactively position themselves as a secure brand will benefit. When making the leap into mobile authentication:

- **Choose a solution that supports multiple authentication options . . .** Adopting mobile authentication is a great choice — but banking landscapes are rarely green fields on which you can implement a completely new system. More than likely, you already have business customers that use some form of MFA for online transactions. So opt for a solution that not only supports mobile methods but also more traditional methods like OTP tokens and smart cards — it makes more sense than reinventing the wheel.
- **. . . and leverage that to offer appropriate options to different customer segments.** Once this flexible, open system is in place, you can tailor the choices you make available to your various customer segments. Offer a mixture of the familiar and the new authentication methods while going about making MFA mandatory for all customers. Use the SMS OTP option as a gateway to get late adopters on board; then, over time, you can gently steer them toward more secure options that represent the lowest cost to the bank.
- **Educate to sell and sell to educate.** If only the technologically most secure and convenient option always carried the day. Until that day comes, combine effective marketing with quality user education efforts to bring consumers into the fold — particularly if the business is unwilling to make MFA mandatory for all. Consumers who are well-informed about the benefits of strong mobile authentication will be more likely to buy into it; conversely, reeling them in through marketing can show them how effective security need not be a terrible burden.
- **Keep your mobile banking plans in mind.** If you're making plans to offer banking services completely over the mobile channel in the future, take a serious look at implementing mobile authentication now. Not only will you have the authentication infrastructure in place to assuage customer fears about the security of banking on a phone, but you will already have gotten a vast swath of your retail customer base accustomed to the mobile authentication concept — and it's no use fighting both of those battles at once.

MAXIMIZE THE MOBILE CHANNEL'S SECURITY VALUE: AUTHENTICATE THE TRANSACTION

Effective banking security, whether through the online or mobile channel, rests on three pillars: strong user authentication; transaction authorization; and risk-based activity monitoring.

Authenticating transactions via the mobile channel works well for online banking, offering customers both security and convenience — and provides a bridge to any future rollout of full mobile banking. The transaction confirmation takes place out of band and thus provides a high level of security. To maximize the security of online banking and best leverage the capabilities of the mobile channel, authenticate the user at login, but also:

- **Authenticate the transaction.** Online and mobile banking security is most effective when users are authenticated both when they log into the banking site and when they complete a transaction.¹⁶ This can take the form of requesting additional authentication to set up new payees, make high-value or high-risk transactions, or simply confirm the list of transactions that the customer wants to make before completing a banking session. For example, ING Bank in the Netherlands distributes OTP calculators with two different OTP seeds; it uses one to authenticate the login and the other to confirm the list of requested transactions before paying them — making a man-in-the-middle attack more difficult. Performing transaction authentication out of band is thus a particular strength of mobile authentication, as it takes the man in the middle out of the picture entirely.
- **Monitor usage patterns to protect customers . . .** Requiring additional authentication for every single transaction may strike consumers and banks alike as too time-consuming and expensive. For this and other reasons, banks like HSBC in the UK are implementing sophisticated risk-based activity monitoring systems — monitoring customers' transaction patterns and requiring additional authentication for those transactions that the analysis engine flags as potentially risky. This kind of layered risk approach is a necessary and valuable way to focus on the transactions that matter.¹⁷ Once flagged, the risk engine then triggers an SMS or voice call to the customer that informs him of the pending transaction and either simply asks him to confirm it or to enter an additional PIN or OTP.
- **. . . and make informed authentication decisions to better serve them.** The development of security measures depends on an assessment of the relative risks of identity theft, fraud, and compromise of account or customer data — and the recognition that organizations need to protect against as yet unknown attacks. The mobile authentication channel provides a convenient and intuitive way for customers to interact with these tripartite defenses. And it can greatly ease the process of, for example, authorizing the occasional unusual transaction — such as a European consumer making a large cash withdrawal on a trip to Singapore. Normally, this either triggers a voice call to the customer to confirm that the transaction is authorized — or the bank blocks the card entirely. OOB authentication coupled with transaction risk monitoring can greatly streamline the consumer experience.

WHAT IT MEANS

MORE CONVENIENT AUTHENTICATION FACTORS WILL SUPPLANT TRADITIONAL TOKENS

The various flavors of hardware and software tokens now on the market work just fine for most consumer-level online banking applications. But the lack of widespread adoption of effective strong authentication in some of the world's biggest banking markets — North America and the UK, for example — indicates an ongoing disconnect between consumers' desire for security and willingness to do what it takes to make that security work.¹⁸ Weak regulations are also a culprit in late-adopting markets: Mass adoption, acceptance, and use of strong authentication for online and mobile banking has been very effective in Europe, South America, and the Asia-Pacific region, whether mandated by regulatory fiat or introduced as an option. Many of these success stories involve the use of hardware tokens or smart cards, which are less convenient than the mobile. And there are some very large implementations of mobile authentication out there: Absa Bank in South Africa counts 1 million Internet banking users who use the mobile phone to authenticate themselves. Most tellingly, when given a choice between hardware tokens and mobile authentication — as some banks in Singapore have done — customers opt for mobile. While the various flavors of mobile authentication are not without their own challenges, on the whole it enhances the convenience of secure online banking and will prove essential to any future widespread adoption of function-rich mobile banking — whenever that happens.¹⁹

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

Authentify	RSA Security
ClairMail	Secure Computing
Deepnet Security	StrikeForce
Diversinet	Valimo Wireless
Fronde Anywhere	VASCO
Gemalto	

ENDNOTES

- ¹ New guidelines on online authentication issued in October 2005 by the Federal Financial Institutions Examination Council (FFIEC) in the US acknowledge that passwords are insufficient as the sole means of security. The guidelines do not mandate any specific technology, but require banks and banking application service providers to establish formal programs for measuring the risk of various online activities and deploy solutions that mitigate those risks. See the October 25, 2005, "[FFIEC Tells Banks To Formally Assess Fraud Risk](#)" report.

- ² Most UK banks have long realized that they must introduce strong authentication for retail online banking. But developing and deploying stronger authentication is taking time, partly because UK banks want an industry-wide standard. In the meantime, about half of the UK's Net users are either complacent or paranoid about online banking security. So while UK Net users aren't as spooked as their American cousins, UK banks still face big communication and security problems. See the August 16, 2005, "[What UK Net Users Think About Phishing](#)" report. One factor that might influence mobile authentication adoption in the UK is that the payments association APACS is recommending that UK banks base their 2FA approach around smart card readers — one of the authentication form factors offering the least in terms of portability — to take advantage of the recent nationwide rollout of, and standardization on, chip and PIN. Source: http://www.apacs.org.uk/payments_industry/new_technology_1_4.html.
- ³ Online fraud and identity theft are growing plagues to eCommerce and are eroding consumers' trust in the Internet. In response, some organizations — especially financial institutions — are evaluating strong authentication solutions to protect customers' accounts and curb account hijacking. The key criteria when evaluating such solutions are ease of use, portability, cost, security, manageability, and cross-channel utility. No one solution will dominate adoption, as organizations will pick different options for different reasons. But Entrust IdentityGuard scores strongly across all criteria and emerges as an especially attractive option. See the March 31, 2005, "[What To Look For In Consumer Strong Authentication Solutions](#)" report.
- ⁴ Some vendors, like nCryptone and InCard Technologies, have solutions that address the problem of needing a separate distribution channel: embedding an OTP generator into a smart card. Banking customers can then use this multifunctional card for several different purposes: The magnetic stripe allows use in ATMs; the smart card chip permits chip-and-PIN payments and credentialing; and the OTP generator enables online banking authentication. These cards, only recently available, have already sparked some pilot projects: For example, in the US, Bank of America will roll these cards out to its online brokerage customers later in 2007 and require its use for some transactions beginning in 2008.
- ⁵ Thirty-five percent of European Net users who don't bank online say that a guarantee of online security would encourage them to adopt online banking. But obviously, it's impossible to protect consumers from all fraud or guarantee that any system is 100% secure. See the June 21, 2007, "[Online Banking Holdouts Still Want Security Guarantees](#)" report.
- ⁶ Strong authentication and consumers are a mismatch. Consumers won't accept anything unless they see simple and cheap solutions that present a real benefit. Improved security or authentication alone is no driver for widespread consumer adoption — even in the light of increased transaction risks. Consumers are not ready to pay for better security or carry a token at all times; they are largely unconcerned about better authentication when doing online transactions. See the April 7, 2006, "[VeriSign Goes VIP](#)" report.
- ⁷ The vendors interviewed for this report all offer one or more of the following: OTP delivery via SMS; OTP generation via a mobile phone soft token; out-of-band transaction authentication; digital signature capabilities; mobile banking capabilities; the ability to coexist with hardware and software tokens on the same authentication system; and additional methods of OTP delivery. No one vendor has all of these, but several come close. Source: Forrester's Mobile Authentication Vendor Product Catalog (<http://www.forrester.com/rb/vpc/catalog.jsp?catalogID=43>).

- ⁸ We conducted a quick survey of phones offered free with a contract by the four largest US wireless carriers in November 2006. All of them are capable of sending and receiving text messages. See the January 24, 2007, [“Match Mobile Channel Capabilities To Customer Goals”](#) report.
- ⁹ For example, in the US, AT&T and T-Mobile charge \$0.15 per received text; AT&T offers bundles that bring the per-SMS cost under \$0.025; Verizon charges \$0.10 to \$0.15 per received text; and Sprint does not charge to receive SMSes. Source: Mobile operators.
- ¹⁰ Despite operator claims of average delivery times of under five seconds and delivery rates well over 99%, one study found that text message delivery failed as much as 5% of the time, and that nearly 10% of all SMS deliveries took more than five minutes to complete. See <http://compilers.cs.ucla.edu/~vids/infocom07.pdf> for the full study.
- ¹¹ In early 2007, ABN AMRO compensated four customers for monetary losses from their accounts due to attackers making fraudulent transactions by exploiting the bank’s “Urgent Payment” feature. The bank had long issued OTP tokens to all of its online banking customers, but fraudsters mounted a classic man-in-the-middle attack. The affected consumers opened an infected email attachment, executing a virus on their machines that redirected their Web browsers to a spoof Web site instead of the genuine ABN AMRO site; users typed the “secret” OTPs from their tokens into the spoof site; the fraudsters captured the OTP and passed it on to the genuine bank Web site, allowing them to impersonate the account owner and giving them full control over the bank account. The customers didn’t notice because the attackers passed the customers’ legitimate, intended transactions on to the ABN AMRO site alongside their fraudulent transactions. Source: <http://www.finextra.com/fullstory.asp?id=16750>.
- ¹² Mobile soft tokens have been implemented in a number of geographies, like rural South Africa, where mobile coverage is spotty; soft token OTPs can be used to authenticate a transaction without requiring that the network be available. However, in more developed markets, Forrester believes that over-the-network mobile payment will be confined to niches like mobile content. Authorizing a payment over the mobile network is usually slower than a debit card transaction, so mobile payment is rarely better than the alternatives, discouraging adoption. Worse, there are still no widely accepted mobile payment standards, and the development of either standards or a clear business model has been bedeviled by infighting between and among banks and mobile operators as well as the sheer technical and legal complexity. The prospects look grim — no one has yet found the “must-have” transactions that will encourage millions of consumers to sign up. See the September 18, 2007, [“The Changing Retail Payment Systems Landscape”](#) report.
- ¹³ We drew our data from two surveys: Forrester’s European Consumer Technology Adoption Study (ECTAS) Q2 2006 Survey, which surveyed 25,447 consumers in the seven markets of France, Germany, Italy, the Netherlands, Spain, Sweden, and the UK; and Forrester’s North American Consumer Technology Adoption Study (NACTAS) Q3 2006 Survey, which surveyed 11,134 households in the US and Canada.
- ¹⁴ Source: Sun Microsystems.
- ¹⁵ Many of today’s handsets already support Java, but unfortunately it’s not like having Java support on your PC: Even the latest handsets’ Java implementations have subtle but potentially major differences, and mobile applications need to be carefully tested for each and every handset and PDA to ensure 1) that they function

at all and 2) if they do, that they do so reliably, securely, and as intended. Also, supporting customers trying to download or install applications to a mobile device can easily turn into a nightmare. The first difficulty lies in deciding whose problem it is to solve. Assuming this hurdle has been overcome, there remains the issue of handset difference: The support provider needs to be able to guide the customer through the troubleshooting sequence for that customer's specific device. See the June 21, 2006, "[Function-Rich Mobile Finance In Europe: Not Ready For Prime Time In Retail Banking](#)" report.

¹⁶ Certain changes or transaction types may warrant additional checks, such as telephoning the customer to verify a transaction, or requesting faxed confirmation. The criteria for classifying a transaction or sequence of events as high-risk will differ between banks. For example, banks that do not use any kind of two-factor authentication using random one-time passwords to confirm transactions may consider it high-risk if a customer transfers even a small sum of money to a third party not included on an approved recipients' list, particularly if that customer has not made any such transfers before. See the January 4, 2006, "[Online Banking Security: Give Customers More Control And Reassurance](#)" report.

¹⁷ Start with risk analysis to guide your authentication decisions. If we are to avoid deploying expensive security technologies that greatly inconvenience customers, we must both target and layer security protections. Remember, convenience is the single most important reason for customers' use of online financial services — and will remain so, even as concerned customers place a bit more emphasis on security. Determining the appropriate authentication method requires considering both the frequency and the intrinsic value of the activity. And high intrinsic value means either high dollar value or high sensitivity of information handled. See the June 22, 2006, "[Strategies For Combating Online Fraud](#)" report.

¹⁸ Eighty-three percent of online banking customers claim that they are willing to use more than just a username and password combination for online account access if it improves the security of their account and identity. And 74% say that additional online account and identity security features will be important factors the next time they choose a financial provider. See the June 29, 2005, "[Bank Of America's Strong Authentication Will Protect Online Customers](#)" report.

¹⁹ Psst — have you heard? Mobile banking is the next killer application. While early pioneers with first-generation mobile platforms got burned back in 2000 with low consumer adoption and not-ready-for-prime-time technology, this time is going to be different! Well, at least that's what the marketplace hype would have you believe: Mobile platform vendors and carriers want you to think that the time for mobile banking is now. Forrester hasn't seen buzz like this since aggregation vendors caused a panic among financial firms back in 1999. But here we are again. Same hype, different topic. We hate to rain on this parade, but here's the reality: Today's consumers still aren't very interested in mobile banking. Before putting a mobile offering at the head of the development queue, eBusiness banking execs should sit patiently on the sidelines and wait to see if the early leaders succeed in growing adoption and delivering a solid ROI. See the September 18, 2007, "[Raining On The Mobile Banking Parade](#)" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

For a complete list of worldwide locations, visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.