

From Mobile Phones to Anywhere ATMs: How Security Technology Enables Mobile Banking



www.yankeegroup.com

by Jon Paisner and Phil Hochmuth | November 2008

Executive Summary

The global connectivity revolution is transforming the way consumers access and interact with their financial services accounts. Mobile is an enabling platform for consumers, whether they are physically located in an emerging market such as Latin America, Pakistan and Africa, or in a developed economy such as the United States or Western Europe. Mobile provides consumers without the access to brick-and-mortar or broadband internet connections to complete financial transactions for the first time. The mobile channel will enable financial institutions to add millions of customers while increasing revenue through bill payment and money transfer initiatives both domestically and internationally. In the developed markets such as the United States or Western Europe, financial institutions can use mobile as another channel to create stickiness, reduce churn and decrease operating expenses by migrating customers away from the IVR and one day generate revenue. Due to the inherent differences among not only the customer bases but the financial and mobile infrastructure, we will differentiate the types of applications, adoption drivers and characteristics of the developed and developing markets throughout this Yankee Group Report.

In the developing markets, short message services (SMS, also called text messaging), unstructured supplementary service data (USSD) and SIM-based applications are the primary mobile banking channels, whether a consumer is receiving an alert or paying a bill. Even though SMS has inherent limitations in the number of characters and the richness of the customer experience, a Java or browser experience is still not an available option due to the lack of consumers with data packages and slow network speeds. Since SMS-, USSD- and SIM-based applications are ubiquitous, the mobile channel is viewed as a

way to drive adoption of banking services for consumers, which in many cases were inaccessible due to low broadband penetration and the lack of brick-and-mortar branches in many of the smaller towns and villages. For example, in Latin America where mobile banking through the SMS channel began as early as 2000, the penetration of bank accounts is only 31%—with only Chile, Brazil and Colombia exceeding the average. When comparing this against a mobile penetration of 57.5% and a total population of 575.4 million residents in the Latin American region, the mobile channel provides access to the financial accounts and information for an additional 151.7 million residents according to Yankee Group and World Bank data (see the June 2008 Yankee Group Report *Anywhere Banking: Technology and Attitudes Surrounding Mobile Banking in Latin America*). Even though SMS has deployments dating back to earlier this decade, it does not provide secure transactions for consumers and financial institutions. USSD or a SIM-based deployment have been used in developing economies and providing a much higher level of usability and security.

In the developed markets such as Western Europe and North America the adoption of mobile banking services will be quite different as banks do not view mobile as a channel to open new accounts but to reduce operating expenses such as IVR costs as well as the differences in mobile handsets and network speeds. Due to the differences among the adoption of mobile banking services, the product and deployment strategies must be aligned to deliver a different value proposition to a different type of consumer, one that has a number of financial services accounts and access to 3G broadband speeds over the mobile channel.

Continued on next page

This custom publication has been sponsored by Fundamo.

© Copyright 2008. Yankee Group Research, Inc. All rights reserved.

This Yankee Group Report is published for the sole use of Yankee Group clients. It may not be duplicated, reproduced or transmitted in whole or in part without the express permission of Yankee Group, Prudential Tower, 800 Boylston Street, 27th Floor, Boston, MA 02199. For more information, contact Yankee Group: info@yankeegroup.com; phone: 617-598-7200. All rights reserved. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice.

Executive Summary (continued)

These developed markets will use a multichannel approach, including both SMS and Java or WAP browser experiences (see Exhibit 1). SMS will be used for information alerts and balance inquiries and a fuller, richer experience will be used for transactional and cross-selling interactions. However, the need for secure mobile banking transactions is a worldwide requirement not blurred by regional distinctions or regulatory requirements.

No matter where in the world mobile banking is being rolled out and regardless of the channel (SMS, browser, USSD, SIM or Java), one thing remains the same: Security is the number one

priority of both consumers and enterprises. Even as mobile banking requires a regionally differentiated strategy for SMS versus browser versus Java client, a secure transaction between a consumer's mobile phone and his or her financial institution is vitally important. Without a compelling secure session between the consumer and his or her financial institution, these services will never reach mass adoption. This report focuses on the measures necessary to secure sensitive information and protect against fraudulent transactions without hindering the consumer experience for mobile banking services.

Exhibit 1
 Characteristics of Mobile Banking Criteria in Emerging and Developed Regions
 Source: Yankee Group, 2008

Informational	Transactional	Promotional
<ul style="list-style-type: none"> • Balance/transaction alerts • Advertisements • All markets will utilize 	<ul style="list-style-type: none"> • Bill payment • Remittances • Balance transfer • Generates revenue for banks in all regions 	<ul style="list-style-type: none"> • Sell travel insurance based on location • Click-to-purchase or click-to-call option • Only in developed regions
Ideal Channel: SMS	Ideal Channel: SMS, USSD and Java	Ideal Channel: WAP and Java

Table of Contents

I.	Situational Security	3
	Consumer Communication Channels	3
II.	Mobile Transaction Security Matrix	4
	Putting It All Together	5
III.	Back to the Future: From Sessions to Messages	5
IV.	Conclusions and Recommendations	7

I. Situational Security

The security requirements for a mobile banking infrastructure are dictated by the type of interaction or transaction the bank wants to make, in conjunction with the communications channel being used. Taking this approach, these factors can be put into a grid we'll call the mobile transaction security matrix (see Exhibit 2).

The mobile transaction security matrix analyzes the three predominant mobile interaction types banks have with customers:

- **Informational:** Alerts, advertisements, marketing and promotional information
- **Transactional:** Exchange of funds, in terms of paying external parties from an electronic bank account; transfer of funds among accounts; payments of fees by a customer to a bank or banking partner
- **Promotional:** Similar to informational, but with the possibility of a tie-in to a transactional event—offerings and promotions with a click-to-purchase option tied to them

Consumer Communication Channels

The cross-section of this matrix analyzes the five dominant communications channels used in mobile banking transactions. These include:

- **SMS** provides ubiquitous reach across the globe between all handsets and carriers. The interconnection agreements in place provide any consumer access to any sort of alert, transaction or promotional item. But SMS has inherent limitations. Because it is designed to be the lowest common denominator with

ubiquitous access, the security protocols are limited and SMS only allows 160 characters in each message. This limits the types of applications that can be conducted while still providing a pleasurable consumer experience.

- **Wireless application protocol (WAP) browser, or web browsers** common to most internet-enabled cell phones and smart phones. These transactions can be thought of as the internet on your mobile phone. Depending upon the network and the amount of graphics loading on the web page, the consumer experience can be very poor. The functionality is smoother than SMS, but it can often take many clicks to navigate to the appropriate section of the web site to complete your banking transaction.
- **USSD** allows for short codes to be entered on the phone that will activate on trigger-specific banking transactions. These short codes are preceded by an asterisk to indicate that a USSD command follows (e.g., dialing “*598*1#” to initiate Barclay’s “Hello Money” service). The advantage of USSD is that it does not provide the same 160 character limitations. However, by forcing consumers to learn short codes this is not as easy to use as an application or WAP browsing session.
- **SIM-based applications** are available as one of the options under the basic menu structure of any GSM phone. Consumers complete banking transactions by following an easy-to-use menu—prompts (similar to existing phone functions—like sending a text message). This functionality is intrinsically available on all phones, but does require mobile operator participation.

Exhibit 2
The Mobile Transaction Security Matrix
Source: Yankee Group, 2008

	SMS	WAP	USSD	SIM	Java Client
Informational					
Transactional					
Promotional					

Ideal	More Adequate	Adequate	Less Adequate	Unsuitable

- **Java client**, the online equivalent to one-one-one interactions between a customer and bank customer service representative. These clients are downloaded to mobile devices and used exclusively for executing transactions with a financial institution. The client is tailored specifically for each handset, network and operator, giving the end user a very rich experience. The problem is that without an unlimited data package, this is not a cost-effective way to complete financial transactions. Throughout the developing world, this is not a strong option based on limited handset distribution and the penetration of mobile data packages. But when contrasted with the developed world, this is going to deliver the fullest consumer experience through a smart phone device.

II. Mobile Transaction Security Matrix

From the weakest channel to the strongest, the mobile banking communications channels begin with the SMS format, step up to the stronger WAP and USSD method, and peak with Java-based client applications and SIM applications. SMS infrastructure is not set up to secure end-to-end transactions. Texts can traverse multiple carrier networks, encryption is not available, and integrity of the message path and payload are unverifiable. On the other hand, texting is one of the cheapest, easiest ways to communicate with customers on a large scale, but with an individual, personal touch. Texts to a mobile phone are viewed very quickly from any location, as opposed to direct-(snail) mail marketing, web or print advertisements, or even e-mail marketing. The ubiquity and low cost of SMS also make it an attractive channel.

Browsers (either WAP or internet) provide a deeper level of security. Sessions can be encrypted and secured via tokens, and SSL can be used to protect data in motion. This provides a more secure transaction platform than SMS, while keeping the technology readily available to end users via the standard WAP browser. WAP browser interfaces also require more engagement from end users than SMS. Transactions initiated via WAP require users to open the browser and navigate a WAP browser GUI. Push information to a WAP browser is also only effective when customers are on the financial institution's mobile web site. In addition, banks must complete extra back-end work to

WAP-enable their traditional web interfaces or create parallel mobile web channels for customers. This results in a far greater technology and expertise investment than simply blasting out texts.

The use of unstructured supplementary service data (USSD) is a gateway that does not store any personal information on the handset. Once an encrypted mobile banking session is complete, all information is wiped from the memory of the handset and the network and only remains in the bank's secure server. Instead of secure, personal information remaining encrypted upon the SIM, USSD is a valuable alternative to ensure secure information cannot be stolen from the handset or network.

In addition, with an unstructured data system you don't have the inherent limitations of SMS such as 160 characters but the ubiquity of access across all handsets. This is important because consumers in emerging markets do not have data packages and USSD sessions are often not billed. SMS without encryption is not secure enough to facilitate these transactions between the bank and a consumer over the mobile network. USSD should be viewed as a viable alternative channel to complete transactions such as bill payments and balance transfers.

Java clients are at the high end of the secure mobile banking matrix. These applications are purpose-built by financial institutions to do one thing well, and only that one thing: execute secure transactions on the mobile phone, exclusively with that bank. The concept of Java clients for mobile transactions is similar to the single site browser (SSB) concept emerging in the PC-based banking realm, and analogous to iTunes or other web-enabled commerce applications. The Java client allows only access to the financial institution's transaction servers. Security is embedded in the client, usually with payload encryption and SSL channel encryption.

However, the development and support effort that's required of a large-scale Java client infrastructure makes the technology overkill for less suitable transactions that do not require the highest levels of security. Pushing advertisements or marketing promotions to a mobile phone is akin to cutting butter with a high-end Japanese chef's knife—it's too much tool for the job. Most Java implementations do not allow access to the SIM card at this stage.

Subscriber information modules (SIMs) in mobile phones are the lynchpin technology for mobile operators in managing the identity of their GSM handset user base. These chips support a complex infrastructure of cryptographic data exchange, whereby operators can verify the identity of subscribers, track their locations, and account for consumption of services. At its core, the SIM is a 128-bit, or even at 256-bit, encryption token with the ability to store nearly uncrackable scrambled data. The mobile banking industry and the information security industry in general are realizing the SIMs powerful potential as a tool for securing multiple types of secure transactions.

Besides storing International Mobile Subscriber Identity (IMSI) and authentication key data, SIMs can be used to encrypt, store and process a variety of sensitive data. For example, vendors are looking to the SIM as a convenient, and in some markets, ubiquitous platform for two-factor authentication to enterprise networks, applications and others systems. In such a scenario, systems could send one-time passwords or challenge/response questions to an end user's mobile phone, which enable the devices to act as smart cards, similar to RSA tokens or fobs.

SIM applications are scripted code loaded on a SIM card (either over the air or at personalization) and accessible through the menu structure on the phone. The advantages of these types of applications, from a security perspective, are that they enable direct, secure access to the cryptographic keys on the SIM.

Financial institutions, carriers and mobile banking infrastructure vendors are all starting to recognize the potential of the SIM, and are looking at ways to leverage these capabilities on the endpoint. To provide a more secure mobile banking environment for their customers, banks are approaching the SIM as a networked, readable/writeable ATM card. The powerful cryptographic features of SIMs are perfect for storing sensitive data such as bank account numbers and PINs, transaction records and other data. More advanced usage of the SIM could include scenarios where an application running on a phone can verify the location of the end user via location area identity (LAI) data stored on the chip. To tap into this power on the SIM, mobile banking technologists are writing phone-based applications that use the SIM as an integral part of their operation. Phone-based mobile banking applications (often written in Java) that can pass data to, and access it from, the device's SIM card (or even applications residing on the SIM itself) are part of this approach.

Putting It All Together

Mobile banking goes beyond basic banking functions. Promotions, marketing and sales opportunities are also part of the transaction landscape. However, banks with mobile service offerings will live and die by the strength of their security for the most sensitive transactions. So how do financial institutions secure the most critical funds transfers and payment transactions? To do this, banks should look to a security architecture they've known for years, but may have never considered applicable to the mobile world (see Exhibit 2 on page 3).

III. Back to the Future: From Sessions to Messages

Mobile banking security architectures must further evolve to bring mobile banking to the same level of security as ATM transactions, or even face-to-face interactions with tellers. Many technologies exist to secure online and mobile banking transactions. The faceless, any-to-any nature of the IP networks, carrier SMS networks and the internet requires banks, mobile operators and service providers to replace the loss of inherent trust which exists in traditional electronic banking transactions.

In such an architecture, trusted zones between the ATM machine, the switched network for transmitting transactional data, and the back-end mainframes or servers guarantee integrity of electronic banking transactions. This architecture enables banks to:

- Precisely discern the origin of all banking transaction messages
- Deliver with the guarantee that they have not been modified in transit
- Deny the ability for customers, or other institutions, to dispute the source of messages they send

Web banking shifted the transaction architecture to stateful sessions—where TCP/IP and HTTP communications are established between a customer's web browser and the bank's server. In this architecture, data transmissions depend on each other to create the stateful connection—an open tunnel—through which customers interact with the bank. When business finishes, the web browser is closed along with the tunnel. The security weakness here is that if a session is compromised, an attacker

has a wide-open portal into a customer’s accounts and activities, as opposed to a message-based infrastructure where an attacker would have to compromise a series of discrete, unconnected messages to execute a fraudulent transaction (see Exhibit 3).

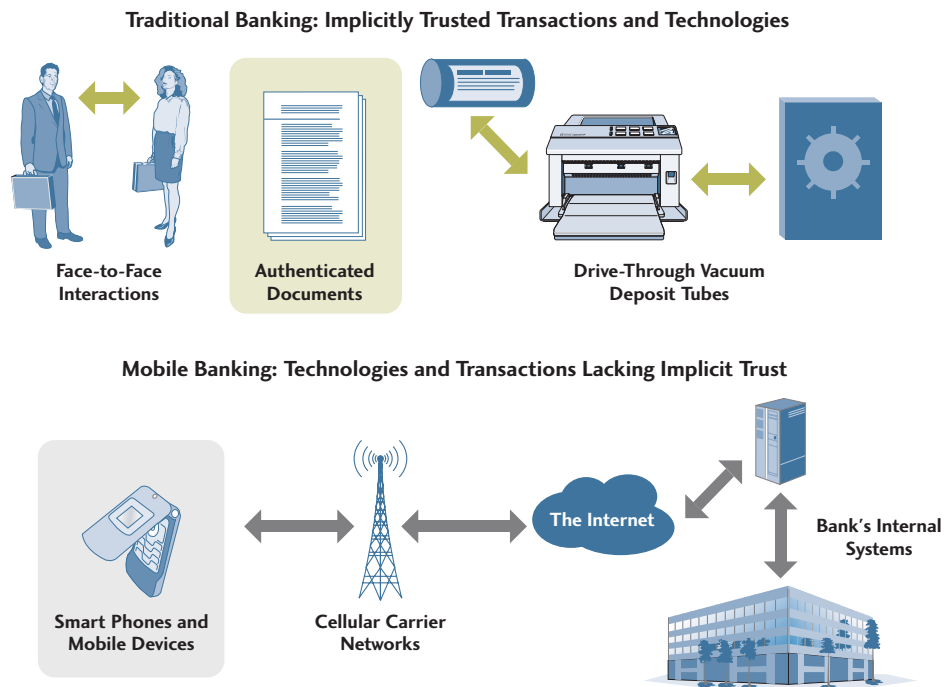
The potential limitation of some mobile banking architectures is that they recreate the desktop, session-based web banking experience on a mobile device’s WAP browser. This method provides the user no security as WAP-based sessions are open to the same vulnerabilities as PC-based web banking. An alternative approach is to return mobile banking back to the message-based architecture roots. Part of that architecture uses hardware-based encryption to secure message payloads, such as single-purpose encryption cards embedded into ATM or point-of-sale (PoS) machines. Session-based or browser-based mobile banking relies on software-based encryption, which is less robust than hardware-based encryption. This is where the SIM card on a mobile device could be leveraged. The SIM smart card in cell phones and smart phones can provide a very high level of hardware-based encryption—256-bit Advanced Encryption Standard (AES), which is difficult, if not impossible, to execute on the limited processing and OS resources of a cell phone. This brings the encryption level of a mobile banking transaction more in-line with traditional message-based security.

This type of message-level encryption, combined with a single-purpose, downloadable application (Java or SIM-based), further replicates the security of ATM-to-bank or PoS-to-bank connections. ATMs perform one set of functions only: manage money withdrawals, deposits, transfers and payments. The Java client, combined with hardware-based encryption, also offers this single-purpose type of experience. By design, this also limits the opportunities for vulnerabilities and attacks on the underlying software. All of this requires multiple tiers of security that can span the various data transmission points, or thresholds, of a mobile banking transaction. One threshold is the handoff from the mobile device (the SIM card on a cell phone) to the carrier network is one transit point. Other thresholds include data handoff points between carrier networks and financial institutions, as well as any required clearing houses (i.e., PIN verification and mobile-to-mobile transaction clearing).

Message-based communications can also provide security for a transaction on every hop or network the message traverses. In browser-based mobile banking, some channel-level encryption exists, such as handset-to-tower links, as well as SSL for internet-based traffic. However, this model depends on the operator of each network hop to provide security for its own leg of the journey. Complete end-to-end encryption and channel security

Exhibit 3
Message-Based vs. Session-Based Security

Source: Yankee Group, 2008



are not guaranteed, especially at the handoff points along the path of a session-based, mobile banking transaction (i.e., between mobile operators and the internet, or the internet and financial institution networks).

A message-based transaction architecture relies on message-level security and encryption where the origin and destination of a message cannot be spoofed, tampered with, or even read by parties other than the sender and receiver. This overrides any weaknesses in any channel encryption technology, or other gaps in the secure path at the handoff points between operators. Unlike session-based communications, an attacker cannot determine the origin or destination of a transaction by intercepting any portion of an HTTP or SSL session stream.

Message-based transactions and security also ensure a more deterministic, reliable type of service. Sessions that are interrupted during critical points of a transaction can cause serious errors during a transaction process. These errors can even result in loss of funds or account errors. In a message architecture, each message provides a discrete set of instructions and data that does not depend on other messages in a transaction stream.

If a connection is interrupted, either by technology failure or deliberate hacking, message-based transactions are unaffected.

V. Conclusions and Recommendations

The infrastructure, communications channels and security standards required to build the secure mobile banking architecture of the future are all ready and just waiting to be put together properly by carriers, financial institutions and ISVs. The following are Yankee Group's recommendations on how organizations with mobile banking aspirations should construct an infrastructure that is secure, reliable and, most importantly, profitable:

- **Use the right level of security for the right transactions.** Security is neither a trivial nor inexpensive technology. For transaction types from basic information to highly confidential, it is critical to apply the appropriate communications channel—SMS, USSD, SIM or Java OS—with the underlying security architecture each channel provides. Let the mobile transactions security matrix be your guide.

- **Consider the security of the network transport layer.** All channels are secured by means of communication layer security. The security for different channels such as SMS, WAP and USSD are all different because the communication layers are all different. But drill-down another layer, and consider the security underpinnings of the devices and applications themselves. Only if a banking application resides on the handset (Java and SIM applications) can application layer security be provided for, which is an additional layer often required by banking applications.
- **Secure data on the endpoints themselves.** Leveraging the SIM as an endpoint cryptography engine, as well as a secure data storage device, will be key for any bank, systems vendor or carrier that wants to be a part of a secure mobile banking infrastructure. Infrastructure vendors and financial institutions must reach out to device makers, as well as carriers, who often control access to the SIM on phones. Including the makers of the SIM hardware itself—the Gemaltos, Oberthurs and Giesecke & Devrients of the world—will also be important for companies writing next-generation mobile banking software that either leverages, or lives on, the SIM.
- **Move to a message-based architecture for the most critical transactions.** Simply replicating a web-based banking security technology on the mobile phone does not make a mobile banking transaction more secure. Strong hardware-based encryption on the mobile SIM—the use of encrypted messages—versus session-based transactions and the single-purpose nature of a Java mobile banking client can bring mobile banking closer to the level of security of traditional electronic banking systems.

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

Prudential Tower
800 Boylston Street
27th Floor
BOSTON, MASSACHUSETTS 02199
617-598-7200 phone
617-598-7400 fax
info@yankeegroup.com

Europe

56 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
44-20-7307-1050 phone
44-20-7323-3747 fax
euroinfo@yankeegroup.com

Yankee Group | the global connectivity experts™

A global connectivity revolution is under way, transforming the way that businesses and consumers interact beyond anything we have experienced to date. The stakes are high, and there are new needs to be met while power shifts among traditional and new market entrants. Advice about technology change is everywhere—in the clamor of the media, the boardroom approaches of management consultants and the technology research community. Among these sources, Yankee Group stands out as the original and most respected source of deep insight and counsel for the builders, operators and users of connectivity solutions.

For 37 years, we have conducted primary research on the fundamental questions that chart the pace and nature of technology changes on networks, consumers and enterprises. Coupling professional expertise in communications development and deployment with hundreds of interviews and tens of thousands of data points each year, we provide qualitative and quantitative information to our clients in an insightful, timely, flexible and economic offering.

Yankee Group Link

As technology connects more people, places and things, players must confront challenging questions to benefit from the changes: which technologies, what economic models, which partners and what offerings? Yankee Group Link™ is the research membership uniquely positioned to bring you the focus, the depth, the history and the flexibility you need to answer these questions.

Yankee Group Link membership connects you to our qualitative analysis of the technologies, services and industries we assess in our research agenda charting global connectivity change. It also connects you to unique quantitative data from the dozens of annual surveys we conduct with thousands of enterprises and consumers, along with market adoption data, comprehensive forecasts and global regulatory dashboards.

Yankee Group Link Research

As a Link member, you have access to more than 500 research reports and notes that Yankee Group publishes each year. Link Research examines current business issues with a unique combination of knowledge and services. We explore topics in an easy-to-read, solutions-oriented format. With the combination of market-driven research and built-in direct access to Yankee Group analysts, you benefit from the interpretation and application of our research to your individual business requirements.

Yankee Group Link Interaction

Our analysts are at your further disposal with data, information or advice on a particular topic at the core of a Link membership. We encourage you to have direct interaction with analysts through ongoing conversations, conference calls and briefings.

Yankee Group Link Data

Yankee Group Link Data modules provide a comprehensive, quantitative perspective of global connectivity markets, technologies and the competitive landscape. Together with Link Research, data modules connect you to the information you need to make the most informed strategic and tactical business decisions.

Yankee Group Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and survey results to your specific needs to produce expert, timely, custom results.

Yankee Group Signature Events

Yankee Group conferences, webinars and speaking engagements offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this connectivity revolution.

www.yankeegroup.com

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel for builders, operators and users of connectivity solutions. For more than 35 years, Yankee Group has conducted primary research that charts the pace of technology change and its effect on networks, consumers and enterprises. Headquartered in Boston, Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific.