

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS MOBILE FINANCIAL SERVICES: RECOMMENDATIONS FOR BUSINESS REQUIREMENTS AND TECHNICAL GUIDELINES

Version 1.0
March 15, 2002

© BITS 2002. All rights reserved.

**BITS MOBILE FINANCIAL SERVICES:
RECOMMENDATIONS FOR BUSINESS REQUIREMENTS
AND TECHNICAL GUIDELINES**

EXECUTIVE SUMMARY	1
Section I. INTRODUCTION	2
Section II. MOBILE APPLICATION BUSINESS GUIDELINES	4
Section III. REFERENCE ARCHITECTURES FOR MOBILE FINANCIAL SERVICES	10
Section IV. NETWORK GUIDELINES	12
Section IV. A. Service Areas and Standards Supported.....	12
Section IV. B. Wireless Transmission Rates.....	13
Section IV. C. Outdoor Wireless Coverage.....	13
Section IV. D. Indoor Wireless Coverage.....	14
Section IV. E. Mobile Terminals/Wireless Devices Supported.....	15
Section IV. F. Wireless Network Usability.....	15
Section IV. G. Security.....	16
Section IV. H. Mobile Support.....	17
Section IV. I. Transparent, Seamless Services.....	17
Section IV. J. Environmental Guidelines.....	17
Section IV. K. Performance Guidelines.....	18
Section IV. L. Service Quality Guidelines.....	18
Section IV. M. Support for Multicast and Broadcast Services.....	18
Section IV. N. Gateway Guidelines.....	19
Section IV. O. Repair, Upgrade and Customer Service Guidelines.....	19
Section V. SOFTWARE SOLUTIONS GUIDELINES	21
Section V. A. Mobile Applications Support Guidelines.....	21
Section V. B. Service Quality Guidelines.....	21
Section V. C. Compatibility with Wireless and Mobile Standards.....	22
Section V. D. Wireless Devices Supported.....	23
Section V. E. Software Usability.....	23
Section V. F. Security.....	24
Section V. G. Transaction Integrity.....	26
Section V. H. Session Management Guidelines.....	26
Section V. I. Software and Operating Environment.....	27
Section V. J. System and Configuration Management Guidelines.....	28
Section V. K. Privacy Guidelines.....	28
Section V. L. Customer Service Guidelines.....	28
Section V. M. Support for End Users Outside Home Areas.....	29
Section V. N. Transparent, Seamless Services.....	29
Section V. O. Software Performance Guidelines.....	30
Section V. P. Support for Multicast and Broadcast Services.....	30
Section V. Q. Gateway Guidelines.....	31
Section V. R. Operational Database Guidelines.....	32
Section V. S. Repair, Upgrade and Customer Service Guidelines.....	32
Section VI. HANDHELD DEVICE/MOBILE TERMINAL GUIDELINES	33
Section VI. A. Mobile Applications Support Guidelines.....	33
Section VI. B. Mobile Terminal Usability.....	33
Section VI. C. Compatibility with Wireless and Mobile Standards.....	34
Section VI. D. Mobile Terminal/Wireless Handheld Device Software Guidelines.....	35
Section VI. E. Mobile Terminal Security Guidelines.....	35
Section VI. F. Repair, Upgrade and Customer Service Guidelines.....	37
Section VII. CONCLUSIONS	38
APPENDIX	39

**BITS MOBILE FINANCIAL SERVICES:
RECOMMENDATIONS FOR BUSINESS REQUIREMENTS
AND TECHNICAL GUIDELINES**

EXECUTIVE SUMMARY

Wireless communications and mobile financial applications and devices are playing an increasingly important role in delivering information and transaction capability to businesses, employees and consumers. These new technologies provide accurate and up-to-date financial data that expedite financial transactions and decision making—even when people are on the move, far from their offices or homes. With the mass deployment of wireless networks supporting large volumes of high-speed data and voice just beginning, it is important for financial services companies to take immediate steps to specify guidelines for secure delivery of mobile financial services. Guidelines are critical to allow the emerging wireless infrastructure to support widespread availability and use mobile financial services with suitable transaction integrity, security, reliability, privacy and usability.

This document, assembled with significant industry input by the BITS Mobile Financial Services Working Group, details business and technical guidelines for mobile financial services that are intended to promote highly reliable, secure, user-friendly mobile financial services. The guidelines are aimed at promoting open, interoperable, standards-based implementations of mobile financial services by vendors and financial services companies. The guidelines establish 15 broad categories of mobile financial services—and others that may be envisioned in the future—that can be easily used over a variety of wireless networks. The guidelines are meant to be used with a wide range of mobile terminal devices and software environments to exchange information and execute transactions.

The guidelines in this document seek to help wireless network operators, software solution providers and mobile terminal manufacturers understand the needs of financial services providers in an end-to-end environment. Financial services companies—with help from multiple wireless network operators, software providers and mobile terminal vendors—can make these services widely available to customers when that end-to-end environment is both reliable and secure. Companies in each of these segments will benefit from:

- understanding the interactions between the wireless network, mobile terminal and applications software and middleware in support of mobile financial services; and
- using the guidelines and information in this document to create products and services that will enable financial services companies to provide mobile applications that are highly reliable, secure, private and widely available.

The BITS Mobile Financial Services Working Group wishes to thank those companies, agencies and individuals who responded to the BITS Request for Information on Mobile Financial Services issued in December 2000, and who participated in the forums and meetings that led to the creation of these guidelines. For a list of their names, please see the Appendix.

BITS MOBILE FINANCIAL SERVICES: RECOMMENDATIONS FOR BUSINESS REQUIREMENTS AND TECHNICAL GUIDELINES

Section I. INTRODUCTION

Installation of wireless networks is growing rapidly. In 1999, 1.4 million wireless local area network (WLAN) nodes were shipped worldwide, and the number grew to almost 5 million in 2000. By 2006, that number is projected to reach 55.9 million, representing a \$4.5 billion market according to a recent Allied Business Intelligence report.

Over the next five years, wireless networks around the world will advance from first- and second-generation wireless technologies, designed principally for voice communications, to more advanced wireless technologies that will readily support data and visual communications. During the same time frame, significant progress in microelectronic technologies will steadily improve the performance, size, display and memory characteristics of handheld, portable computing and cell phone devices. Taken together, advances in networking and portable device technology will create the technology infrastructure that will enable a large number of mass-market mobile commerce applications.

Mobile financial services offered by integrated financial services companies will be among the leading-edge mobile commerce applications offered over present-day and emerging wireless networks. However, mobile financial services will gain acceptance by consumers and businesses only if the technology infrastructure can support these services reliably and at a level of quality sufficient to make them secure, easy to use, widely available and compatible with the varying needs of highly mobile consumers and businesspeople.

At the time of this writing, serious concerns are being raised about the security of wireless networks. Organizations are using WLANs despite immature technology and inadequate security in both handheld devices and the current WLAN standard, 802.11b. Common risks associated with these problems include financial loss from unauthorized transactions, disclosure of sensitive proprietary information, intrusion into the network and service disruptions.

The three-part technology infrastructure for mobile financial services consists of wireless networks, wireless/mobile computing and telecommunications devices, and software products to support delivery of appropriate content to authorized end users. This infrastructure must be highly secure, highly interoperable, and highly adaptable to the changing needs of customers and financial services companies.

BITS' Mobile Financial Services initiative was launched in June of 2000. Its strategic goals were to:

- Facilitate the adoption of wireless technology in the U.S. financial services industry and improve the quality of the provider services that support financial applications.
- Actively engage in dialogue with technology providers to enhance security solutions.
- Influence standards development to ensure that financial services companies' needs are addressed.

- Identify what role, if any, BITS can play to leverage or enhance industry utilities to facilitate wireless transactions.

The BITS Mobile Financial Services Working Group developed this document as part of this mission.

The *BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines* details requirements for the three segments of the technology infrastructure needed for successful implementation of mobile financial service. BITS is making this material available to inform wireless network operators, mobile terminal and handheld device manufacturers, and mobile software solution providers of the standards and business requirements that will need to be met in order for financial services companies to be able to continually improve the level of security of the financial applications they offer to mobile consumers, professionals and workforce constituencies. In addition to providing guidelines for three mobile industry segments, this document includes general information on mobile applications and on applications networks used by financial services companies to support customer accounts, transactions and financial information services.

Financial services companies must implement mobile financial applications in a way that is consistent with their responsibilities as providers of the U.S. critical economic infrastructure. The guidelines are created with this very important role in mind.

For additional information about the *BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines*, contact: Kathy DeWit, Wells Fargo & Co., kathryn.j.dewit@wellsfargo.com; Sam Phillips, Bank of America Corp., sam.phillips@bankofamerica.com; or Jennifer Dickerson, BITS, jennnd@fsround.org.

Core Team

Eileen Bridges, Bank of America
Kathy DeWit, Wells Fargo & Co.
Jennifer Dickerson, BITS
Stephen Dunn, Bank of Montreal
Mike Gawdun, USAA
Scott Hedberg, Wells Fargo & Co.
Faraz Kohari, ABN AMRO
Howard Lemberg, Telcordia Technologies
Marshall McDowell, State Farm Insurance
Susan Mutter, Wachovia Corporation
Sam Phillips, Bank of America Corp.
Max Ruston, Charles Schwab
Dan Schutzer, Citicorp

Section II. MOBILE APPLICATION BUSINESS GUIDELINES

This section describes the main functional guidelines for key mobile financial applications. Many applications are offered by major financial services companies today over the wired networks and software infrastructure currently in place. In offering these applications over wireless networks in the future, financial services companies will continue to provide their customers with levels of security, usability and application performance consistent with the experience that end users have over wired networks.

Financial services companies recognize that wireless networks are subject to bandwidth and capacity constraints different from those that determine the end user's application experience in a wired network. For this reason, financial services companies are willing to tailor financial applications to the mobile environment so that applications can be delivered under realistic conditions with acceptable performance. The overall security and usability guidelines for mobile financial services are, however, equal to or higher priority than corresponding security and usability guidelines for financial services over wired networks. Financial services companies do not want to sacrifice application security or usability when they offer financial services over wireless networks.

Some mobile applications offered by financial services companies will be customer oriented, and others will be employee oriented. The focus of the applications described below is on customer-oriented applications. While some employee-oriented mobile applications will be similar to those outlined below, others will be customized applications that are variations of business applications currently available to employees of financial services companies over wired channels. In general, employees of financial services companies will eventually expect all applications currently available in the office to be delivered over wireless or mobile channels. They will expect to access those customized mobile applications in a way that is similar to normal wired access, and they will expect mobile applications to behave in ways that are quite similar to the corresponding applications delivered over wired channels.

The applications described below are representative of the kinds of mobile services that many financial services companies are now delivering or will want to deliver over wireless channels in the next few years. Mobile versions of these applications, most of which are already provided to customers in other ways, should be a seamless extension of today's financial services offerings, allowing mobile customers access to applications and data at their current locations via portable wireless devices.

Mobile "push" applications, like their counterparts delivered over wired e-commerce networks, are those in which the application provider or financial services company initiates the transmission of information to the end user. The information can be a short advertisement, an event notification or an invitation to use an application. In mobile "pull" applications, the end user initiates the application session by sending a message to the application or content provider.

Account Balance Inquiries and Inventory (Pull). These applications enable a customer to retrieve account balances across multiple financial services companies' product offerings, such as checking or savings accounts, credit card accounts and brokerage accounts. The applications are "pull" applications because they are initiated by customer request or action. Account Balance Inquiries should be provided with highly secure and reliable customer authorization and authentication at the application level, as distinct from the authorization and authentication imposed by the wireless network operator for use of its network.

Transaction Initiation and Execution (Pull). These applications enable a customer to initiate and/or terminate financial account events, or initiate and/or terminate financial product orders or inquiries. The account or product events thus instigated may take place within a single financial services company or across several such companies. Examples of Transaction Initiation or Execution events include, but are not limited to, micropayments, anonymous payments, foreign exchange orders, account balance transfers, security purchases and sales and loan payments. These applications are "pull" applications, and they should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authorization and authentication for Account Balance Inquiries. Transaction Initiation and Execution applications thus entail authorization and authentication of the customer, as separate and distinct from the authorization and authentication imposed by the wireless network operator for use of its network.

Data Message Exchange. These applications, such as short message service or instant chat, enable customers to exchange short messages, typically no more than 50 to 180 characters, with another person or financial services company representative who also participates in or subscribes to the short message or instant chat application. The Data Message Exchange application may be a "push" application, meaning that messages can be pushed from one individual to another with very high probability of successful message delivery in less than one minute. This suggests that the wireless terminal device should either be "always on" or should have an "instant on" capability that allows it to be turned on upon receiving an alerting message. Because of the sensitive nature of the financial information potentially exchanged in a financial services company's Data Message Exchange session, these applications should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution.

Personalized Alerts (Push). These applications allow a financial services company to send personalized alert messages to individuals or large numbers of subscribers, in response to external news or financial events, with the nature and frequency of the personalized alerts for each customer controlled by an "alert profile" maintained by the financial services company. Some alerts will be common to a large number of customers and should be broadcast or multicast to all members of a broadcast/multicast address list. Other alerts will be tailored and delivered to individual customers, based on alert profile parameters that the customer can access and change. Personalized Alert applications are "push" applications that are generally initiated by the financial services company, and successful alert delivery to all customers on the address list should be provided within one to two minutes of initiation of the message push. Because of the push nature of the alerts, prior authentication at the application level is not needed, but the wireless operator should ensure that the alerts are delivered only to the authorized wireless terminals on the financial services company's

broadcast or multicast address list. The push nature of Personalized Alert applications generally means that the wireless terminal should either be “always on” or should have an “instant on” capability that allows it to be turned on upon receiving an alerting signal.

Account Service (Push and Pull). Account Service applications, which can be initiated either by the customer or by the financial services company, allow a customer to apply for new financial services, enable or disable features or options in financial services and personalize financial services. Because these applications entail customer access to profile information and/or manipulation of the customer’s financial service parameters, these data exchanges should be carried out under conditions that support high security, data integrity, and reliability, as with Account Balance Inquiries. Account Service applications should be carried out after appropriate authorization and authentication of the customer, as separate and distinct from the authorization and authentication that is imposed by the wireless network operator for use of its network.

Wireless Information Synchronization. Wireless Information Synchronization applications enable a mobile customer to link to a distant computer over highly secure, highly reliable wireless channels, and synchronize information associated with various application programs between the distant computer and the mobile customer’s wireless terminal. Examples of information that may be synchronized include, but are not limited to, electronic mail messages with attachments, address book contents, and electronic files in selected computer directories or folders. Wireless information synchronization may sometimes be used by financial services companies to let employees or customers have access to consistent information over wired channels (e.g., from an office computer) and over wireless channels (e.g., from a wireless-enabled personal organizer or a notebook computer with a wireless modem). Wireless Information Synchronization applications need high bandwidth and throughput in the downlink (from the network to the customer’s mobile terminal) and the uplink (from the customer’s mobile terminal to the network). Because of the sensitive nature of the information exchanged in a Wireless Information Synchronization session, these applications should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution. Wireless Information Synchronization application sessions will be highly variable with respect to the volumes of information transmitted to and from the mobile terminal for synchronization purposes.

Portal Information Access. Portal Information Access applications enable a customer to access typical financial and non-financial information such as news, weather, sports and stock exchange summaries through a standard browser over wireless channels, and to have that information displayed on the wireless terminal’s screen. Information access will typically be through a default entry page, or portal, that can be selected and/or tailored by the customer. An individual customer’s Portal Information Access session may thus entail access to multiple pages or screen displays, as the customer locates the specific information of interest. A typical Portal Information Access session may involve selection and display of about ten or more screens’ worth of information, with the quantity of information transmitted per screen page depending on the relative fraction of character-mode and graphics content per page.

Aggregation Services (Push and Pull). Aggregation Services applications make consolidated financial and non-financial information available to the customer for online or mobile retrieval. The aggregated information may be assembled by the financial services company prior to the customer's request for data access, in which case the wireless network is responsible for secure, reliable and timely delivery of aggregated data to the customer who requested it. Alternatively, the aggregated information may be assembled electronically in near real time by the financial services company's applications network, in response to a series of menu selections or customized, session-specific commands issued by the customer. Because Aggregation Services applications may entail customer access to profile information, possible changes to the customer's financial service parameters, and access to confidential customer-specific financial information, they should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authentication and authorization for Account Balance Inquiries. Aggregation Services applications thus entail authorization and authentication of the customer, as separate and distinct from the authorization and authentication required by the wireless network operator for use of its network.

Promotion Cross Selling (Push and Pull). Promotion Cross Selling applications, which can be implemented as "push" and "pull" applications, leverage customer interactions with the financial services company to present the customer with one or more opportunities to use or purchase other products or services. From the customer's point of view, Promotion Cross Selling applications appear as extensions of a mobile financial service session that the customer is already engaged in, and customers may wish to resume a mobile application session or initiate a new mobile application session after dealing with one or more Promotion Cross Selling messages. Since mobile application sessions may be supported at varying levels of performance, throughput and security, the wireless network should permit the financial services company and the customer to negotiate session context parameters at session initiation so that the customer gets adequate performance, reliability and security for mobile financial transactions.

Financial Advice (Push and Pull). Financial Advice applications are "push and pull" applications that recommend general or specific courses of action to specific customers, based on external events or a combination of external events and personal profile information. The advice offered over wireless channels will often be advice with a relatively near-term time frame for action. To the extent that this advice is customer-specific and messages transmitting this advice contain confidential customer account details, these applications should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution. To the extent that financial advice pushed to customers is generic or is based on widely available public news and information sources, levels of security and reliability, and application-level authentication or authorization of the customer, may be less stringent.

Bill Presentment and Payment (Pull). Bill Presentment and Payment applications enable a customer of a financial services company to request, via mobile or wireless channels, the assembly of a bill or account statement from a specific company or institution, and its presentation in appropriate form on the customer's mobile terminal. These applications also permit the customer to make arrangements for bill or invoice payment through a credit card,

credit account or other account. Because of the sensitive nature of the financial information potentially exchanged in a Bill Presentment and Payment session, these applications should be provided with highly secure and reliable customer authorization and authentication, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution.

Loan Application/Prequalification. Loan Application and Prequalification applications permit a customer to submit preliminary personal and financial information to a financial services company, subject to later verification, in connection with a loan application. Because of the personal and highly confidential nature of this information, when offered over wireless channels these applications should be provided with highly secure and reliable customer authorization and authentication, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution.

Mobile Commerce (Push and Pull). Mobile Commerce, which can be provided as “push” or “pull” applications, lets financial services companies support business-to-business and business-to-consumer inquiries, transactions and account transfers, as well as information exchanges among multiple financial services companies. These applications may involve Web-enabled catalog browsing, advertising, ordering, payment and credit postings, and purchase confirmation messages. Some Mobile Commerce application messages may contain information that is not confidential (e.g., public Web pages, catalogs, advertisements) and thus can be handled at low levels of security, but other Mobile Commerce messages should be provided with highly secure and reliable customer authorization and authentication because they contain account-specific information or confidential business data. The wireless network handling Mobile Commerce applications should thus support switching and transmission of messages at several levels of security, with several levels of authentication and authorization.

Location-Based Financial Services (Push and Pull). Location-based financial services, which can be implemented as “push” or “pull” applications, enable financial services companies to provide information and other services that are tailored to the customer’s geographic location, based on GPS or other location-identification data transmitted over wireless channels to the wireless network operator and then to the application provider. It is essential for customer location information to be available so that the application provider can inform the customer about locations of nearby offices, agents or ATM machines. Other mobile commerce applications of this type include focused advertisements and location-sensitive message filtering.

E-to-E Marketplace. Exchange-to-Exchange (E-to-E) applications are financial applications that facilitate transactions between businesses and electronic/financial exchanges, and between various financial exchanges. The exchanges are, in effect, electronic clearinghouses that facilitate business-to-business electronic commerce, supply chain management, international trade and invoice payments across multiple financial services companies. Mobile E-to-E marketplace services will facilitate certain E-to-E functions and message exchanges to expedite orders, payments and settlements by transmitting ordering documents, verifications and payment information in standard formats accepted by the exchanges. Because of the high value of many E-to-E transactions and the likelihood that

company proprietary financial and account information will be included in E-to-E application messages, E-to-E applications should be provided with highly secure and reliable customer authorization and authentication at the application level, in a way that is similar to customer authentication and authorization for Account Balance Inquiries or Transaction Initiation and Execution.

Section III. REFERENCE ARCHITECTURES FOR MOBILE FINANCIAL SERVICES

Figure 1 (next page) depicts the reference architecture for mobile financial services supported by a second- or third-generation wireless network infrastructure. After gaining authentication and authorization to use the wireless network, mobile/wireless terminals communicate over the radio access network with a base station transceiver and controller, which are linked to a mobile switching center in the core network. Individual calls or data packets are switched or routed in the core network to the financial services company's applications network, based on the addressing information they carry.

The financial services company's network consists of computer hardware and software running existing financial applications. This existing information infrastructure also contains the company's customer and transaction data, and embeds business rules that define how different parts of the financial company do business with one another, with other financial services companies, and with retail and wholesale customers. The lower rectangle illustrates some of the functions and process modules that would be involved, at the middleware and application levels, in extending financial services to the wireless/mobile domain. Many of the modules and functions illustrated in the lower part of the figure have counterparts or corresponding objects in mobile middleware and applications software running in the mobile terminal, but detailed software decomposition of the mobile terminal is suppressed in Figure 1.

Existing applications and databases containing the financial services company's proprietary business and customer-specific data are shown at the bottom of Figure 1. Mobile financial applications, to be successful, will exploit and adapt existing application code and data. Middleware functions that apply to a large number of common applications are shown at the lower left. Although the figure lists only wireless and data security, many other common middleware functions will be supported in a realistic financial services network. Address resolution, data, messaging and/or content adaptation, or message adaptation to end-user mobile terminals, end-to-end error and sequence checking, and session management are among the middleware functions that should be supported across multiple applications.

From functional and application perspectives, architectures for mobile financial services over second- and third-generation wireless networks are quite similar. The major difference between the two is that third-generation networks will provide much more advanced support for wireless data services, at higher bandwidths or throughput levels. Third-generation mobile terminals could provide support for simultaneous high-speed data and "always-on" capability.

Third-generation wireless networks will also transmit voice in a digital format quite similar to the way that data will be formatted, potentially permitting financial services companies and application providers to integrate voice and data carrier services in delivering mobile financial services. This new integration of voice and data may permit financial services companies to provide mobile applications with voice recognition, voice-enabled navigation of wireless websites, and real-time call center assistance to customers needing help with mobile financial applications.

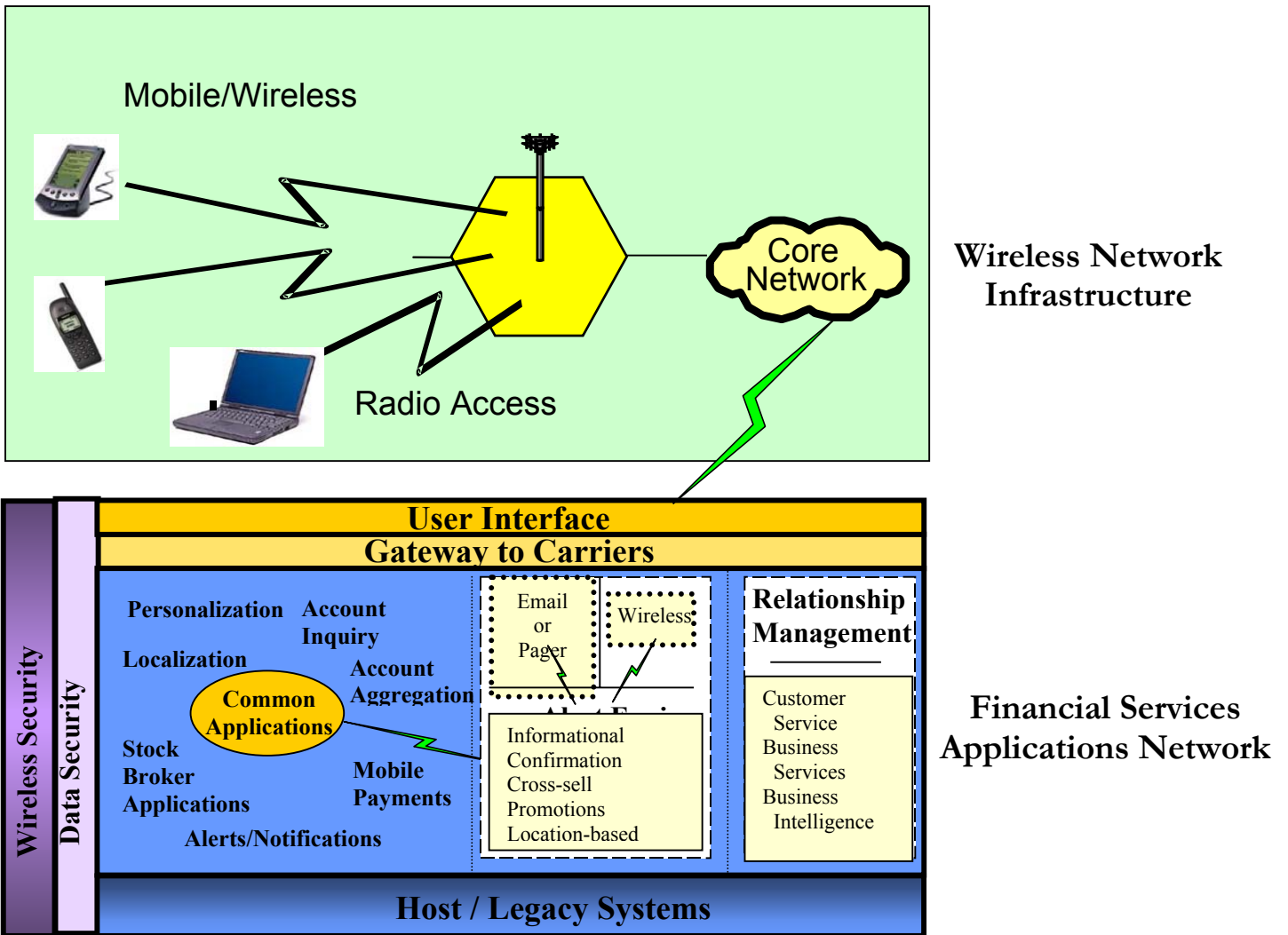


Figure 1. Wireless Reference Architecture and Relationship to a Financial Services Company's Applications Network

Section IV. NETWORK GUIDELINES

This section summarizes guidelines for the wireless networks that will provide communications transport, switching and access for mobile financial services. The wireless network comprises a wireless access network, allowing a customer with a mobile terminal to communicate with a base station using radio transmission techniques, and a core or backbone network, allowing for transmission and routing of individual calls or data packets from an originating area to a destination. The core or backbone network is generally implemented with wired transmission lines between the base station and the core network, and with wired connections between the switches or routers in the core.

The guidelines in this section apply to the wireless access network and to the core network.

Section IV. A. Service Areas and Standards Supported

For mobile financial applications to be useful to end users, businesses and financial services companies, it is important for the underlying communications services to be widely—and ultimately ubiquitously—available in North America. While it may be several years before individual wireless data services reach the vast majority of North American end users, financial services companies supporting mobile applications need to understand the geographic scope of wireless carriers' services. Thus, wireless network operators should supply financial services companies with up-to-date, accurate coverage information for individual wireless voice and data services. This coverage information should specify the maximum and average bit rates that are achievable, under normal operating conditions, from one geographic area to another, so that financial services companies can appropriately plan and implement their applications. The coverage information supplied by each wireless network operator should also include the highest bit rates to which each operator would be willing to commit in a service level agreement, with one bit rate corresponding to the highest bit rate that can be achieved in 99% of the coverage area under normal operating conditions and the second bit rate corresponding to the highest bit rate that can be achieved in 75% of the coverage area under normal operating conditions.

Wireless network operators shall be willing to commit to some form of coverage and service guarantees, possibly in the form of service level agreements specifying the conditions under which maximum, average and minimum bit rates, or performance and availability, can be achieved in each geographic area.

It is expected that the wireless networks used for mobile financial services be based on widely implemented and supported standards to maximize interoperability and usability as mobile customers travel from one service area to another and from one network operator's service territory to another's service territory. Interoperability is needed at the transport and service levels. As a consequence, the wireless networks used for ubiquitous financial services should be based on widely accepted and widely implemented standards for wireless transport and mobility management. Implementation of these standards by each wireless network operator should support:

- interconnection of the wireless access network to a variety of core networks;
- interconnection of a carrier's wireless network to the core network of another network operator;
- wireless data services for transmission of mobile financial applications;
- simultaneous voice-data capability;

- mobility by end users while they are using mobile financial applications; and
- widely available access to mobile financial applications, including access from areas other than the customer's home area and from areas that are outside the wireless network operator's service territory.

Section IV. B. Wireless Transmission Rates

This section addresses wireless capacity guidelines for mobile financial services in terms of channel throughput or wireless transmission rates.

Over the long term, it is expected that transmission rates per active end user of at least 144 kb/s will be achieved for access to a range of mobile financial services. Lower transmission rates will produce lengthy delays if applications use graphical user interfaces or rely on large display areas.

In the near term, wireless transmission rates of 10 kb/s to 20 kb/s will be widely available, and it will be possible to tailor applications to limited available bandwidth—either by efficiently coding the information that is transmitted or by restricting the scope and variety of the applications offered. Although some financial applications can be offered on an interim basis over these limited-bandwidth channels, wireless network operators should make higher transmission rates much more widely available to improve the usability of the financial applications that can be delivered to end users. Ubiquitous wireless coverage at higher transmission rates will allow financial services companies to support applications with lower transmission delays and will also enable services to be provided to mobile terminals with larger display areas without sacrificing response times or readability.

Wireless network operators wanting to support mobile financial services should provide financial services companies with wireless transmission rates in the near term of at least 20 kb/s across all of their service areas. Near-term transmission rates of about 128 kb/s would be preferable, at least for stationary or slow-moving customers, with an increase over the next few years to about 144 kb/s per active end user for end users traveling at highway speeds. Wireless networks should support even higher speeds of 300 kb/s to 400 kb/s in the next five years for end users who are moving at low speed or are stationary.

Financial applications that are now or could be implemented in the next few years over wireless networks with limited transmission rates of 10 kb/s to 20 kb/s include, but are not limited to: simple account balance inquiries, account service requests, transaction initiation and execution, portal information access, and mobile commerce transactions. The applications possible in a session of reasonable duration over these limited-bandwidth channels can be implemented with a small amount of text input and output (i.e., no complex graphics are needed), and realized in a small number of messages exchanged by the mobile terminal and the application server.

Section IV. C. Outdoor Wireless Coverage

While much of the initial demand for mobile financial applications may be concentrated in large metropolitan areas, financial services companies have a strong interest in and need to support access to financial information and transactions in suburban and rural areas. Wireless network operators should be prepared, therefore, to provide wireless data service coverage in non-metropolitan areas as well as in large urban areas. They should be prepared to inform financial services companies about the nature of the wireless data services that will be supported in suburban and rural areas. In particular, wireless network operators should be prepared to provide technical details of the wireless data services they will support outside metropolitan areas, including:

- the maximum and average bit rates per user that will be supported;
- the coverage areas within which those bit rates will be supported; and
- the wireless standards that will be used for wireless access, transport and mobility.

In the interest of expediting widespread access to mobile financial applications, it should be noted that wireless network operators need not use the same wireless standards and technologies in densely populated and sparsely populated areas in the near term. Wireless carriers can, for example, offer a set of data services based on one family of wireless standards in urban areas and, for an interim period, offer another set of wireless data services, based on a second family of wireless standards, in less densely occupied areas. When support for mobile financial applications is offered in this way, however, the two sets of wireless data services should be available from a common handset or mobile terminal. The customer should not need separate handsets or mobile terminals to access the wireless data services available from a single carrier in different geographic areas. Rather, the customer's experience should be similar to the experience of today's wireless voice users, who can access CDMA (IS-95) services in areas with CDMA voice service and analog wireless voice in those geographic areas where CDMA service is not available.

The major wireless standards on which mobile financial services will be implemented in the near term will probably be second-generation cellular and wireless data offerings now widely available in many parts of North America. Over the long term, the major standards on which mobile financial services will be based will include the major third-generation wireless standards in use around the world. These long-term standards could include, but will not be limited to, CDMA2000 and W-CDMA specifications and standards issues by ANSI, T1 and ITU.

In the near term, the secondary sets of wireless standards that may be used for mobile financial services in less densely occupied areas could include CDPD, Mobitex, Motient and other wireless data standards. Over the longer term, as third-generation standards are implemented in North America, the secondary sets of wireless standards that may be used to fill out coverage in less densely populated areas could include IS-136 TDMA, GSM/GPRS and CDMA 1XRTT.

Section IV. D. Indoor Wireless Coverage

For wireless financial applications to be useful to the vast majority of office-based customers, the wireless data service infrastructure on which they are built should provide acceptable indoor coverage, with low probability of outage or error. Wireless network operators should therefore design their networks and services so that sufficient received signal strength can be detected inside typical urban and suburban office buildings. Designs for indoor coverage typically require a sufficiently high minimum transmitted power at each base station and/or some mechanism for amplifying or repeating wireless signals indoors, so that data streams with sufficiently low error rates can be constructed at the receiving end.

Wireless network operators should inform financial services companies about what specific measures they are taking to ensure adequate indoor coverage and error-free reception for the wireless data services that will be used to deliver mobile financial applications to customers. In general, financial services companies will want acceptable indoor coverage provided for more than 98% of the occupants of urban and suburban office buildings.

Wireless network operators should coordinate outdoor, wide-area network coverage and indoor wireless coverage so that mobile applications are supported continuously and seamlessly when a customer moves between outdoor and indoor areas.

Section IV. E. Mobile Terminals/Wireless Devices Supported

Financial services companies are interested in delivering mobile applications to a range of business, consumer and workplace customers who are using a range of mobile terminals and wireless access devices. In addition to implementing widely accepted wireless and mobility standards, wireless network operators should ensure that their data services can be used by a fairly broad range of mobile terminals so that customers are not limited in their choice of wireless access device, screen size or mobile terminal manufacturer.

Financial services companies also want to offer mobile applications that are stable and predictable but that can evolve to take advantage of new network and terminal technologies. At the same time, they do not want to force customers to purchase and use new mobile terminals to keep pace with every incremental improvement in wireless technology. Wireless network operators serving the financial services industry should therefore be prepared to specify, for each mobile terminal type provisioned by the network operator for mobile financial services, the minimum time interval that the operator's network will continue to support wireless data services to the terminal.

Section IV. F. Wireless Network Usability

The mobile financial services described in Section II, when implemented between a mobile terminal and the applications network of a financial services company, should be backward compatible and easily usable by customers over a large number of wireless networks, with many types of mobile terminals, in nearly any location. Customers shall not be required to go through an aggregator to access the services. The wireless network operator should support application usability by providing ubiquitous access to the high-speed wireless data channels noted in Section IV. B. by installing sufficient base station capacity to accommodate localized network loads in high-traffic areas, and by eliminating coverage gaps. Network operators should plan and implement their networks so that high-speed data coverage is not limited to low transmission speeds near the edges of wireless cells. Network operators should also ensure that radio-frequency interference from some customers does not disrupt completion of financial services sessions by other customers.

Other aspects of wireless network design that will influence usability of end-to-end financial applications include authentication and authorization intervals for the mobile terminal, roaming support, and ease of navigation from one source of content or applications to another.

End-to-end authentication and authorization of customers will generally be built on top of wireless network services with separate authentication and authorization procedures for mobile terminals. To limit delays for application session initiation, wireless network operators should make sure that time intervals for authentication, authorization and channel access for wireless data services are limited to no more than one to three seconds under conditions of normal network load. Wireless network operators are also encouraged to implement interconnection agreements with one another and mobility management procedures so that users of mobile financial services can be rapidly authenticated and authorized for use of appropriate wireless data services even when they are outside of their home areas.

To the extent that wireless network operators are also provisioning agents for the mobile terminals that customers of financial services companies will use, those operators should examine the mobile terminal usability guidelines in Section VI for terminal design or functional criteria that will promote application usability.

Section IV. G. Security

The wireless networks that carry mobile financial services should offer to providers of financial applications extremely high security, reliability and data integrity to protect the privacy and security of highly confidential financial data, transaction details and account/password information that may be transmitted over wireless channels. Long-term, security should be supported by an overall end-to-end security architecture that extends from the mobile terminal or handheld wireless computing device, through the wireless network, and ultimately through the financial services company's applications network.

Certain mobile financial services will deliver public information to mobile end users, similar to the information that might be supplied by a public website or information portal. While the delivery of public information does not, by itself, imply a need for end-to-end encryption, many mobile financial services will involve a mix of public, nonconfidential information such as merchandise or information catalogs, and confidential information such as credit card and/or account numbers. Credit card and transaction information will, in general, benefit significantly from secure encryption between the end user's terminal and the transaction database or website. Thus, the wireless carrier's network should offer sufficiently high bandwidth and low response time to permit use, without unreasonable delay or performance degradation, of end-to-end security mechanisms enabled by encryption keys or digital certificates that are exchanged between application endpoints before secure transactions are executed.

One important consequence of the security scenario described above is that the wireless network operator should permit an end-to-end security solution to be imposed at the mobile application level. The wireless network should not expose any transaction or identifying details of the information flows for secure end-to-end mobile applications. This means that the individual customer's identity, all transaction records, all passwords, and all authentication and authorization sequences should pass through the wireless carrier's network intact, without decryption. It should not be possible to record and decode this confidential information, either by listening to wireless channels with commercial radio frequency scanners, by tapping into wired portions of the network operator's core network, or by recording packet sequences or information that is stored temporarily in gateways or switches that are part of the wireless network.

Because the technology is not readily available to implement these guidelines, some financial services companies may choose to implement interim security solutions without end-to-end encryption to support initial offerings of mobile financial services. Approaches for near-term security solutions of this type should be based on risk assessment and technology availability. Since different financial services companies may make different security choices near-term, the wireless carrier's network should be able to accommodate a range of security architectures, including end-to-end encryption, without adversely affecting mobile application performance or the privacy of customer or transaction information. Furthermore, given the limitation of current technology, some end-to-end encryption options may actually pose a higher risk.

Section IV. H. Mobile Support

Mobile support is essential for mobile financial services, for the applications should be available to people who are in motion at speeds up to typical highway speeds. On some types of public transportation, such as trains, it may be highly desirable for wireless network operators to implement wireless data services that can operate when the end user is traveling at speeds exceeding typical highway speeds.

Effective mobile support for mobile financial applications implies that service and session continuity be maintained while the customer is in motion and moving through geographic areas served by multiple network operators and transmitting antennas (base stations) and by multiple switches. To accomplish this, the wireless network operator should implement procedures to hand off sessions or calls from one network element to another as the end user moves.

Wireless network operators should implement hand-overs in a way that supports session continuity and integrity for mobile financial applications, even when financial application users move from one wireless network to another, or one wireless operator to another. Security, privacy and usability of financial services and information should also be maintained as wireless network operators implement roaming support.

Because of the critical nature of the information being delivered to and transmitted by end users as they exercise mobile financial applications, it is important that the percentage of dropped data calls or sessions that occur be less than 1%, as long as the customer is moving at a speed that is less than the normal speed for the type of transportation being used.

Section IV. I. Transparent, Seamless Services

The network should support mobile financial services in a way that gives the applications the same appearance from one geographic area to another. Input sequences to initiate financial applications on a given mobile terminal should not depend on the customer's specific location, nor should the initiation sequences (key strokes, button clicks, alphanumeric character sequences, etc.) depend on the specific wireless technology carrying the application and associated data.

There may be some variation in input sequences from one type of wireless terminal to another.

While a customer is using a particular application, the control sequences or commands needed to execute specific actions also should not depend on the customer's specific location, though there may be some variation in mid-session control sequences or commands from one type of mobile terminal to another.

The initiation sequences and mid-session control sequences used to activate and execute all financial applications should be independent of the customer's location.

Section IV. J. Environmental Guidelines

The wireless network should be engineered and implemented in such a way that expected variations in environmental conditions do not noticeably affect the usability or performance of mobile financial

services. The availability and coverage characteristics of wireless services, for example, should not be noticeably degraded by adverse weather or seasonal variations in foliage.

Section IV. K. Performance Guidelines

Mobile financial applications should meet high-level wireless network performance requirements.

Reasons for this include, but are not limited to:

- the sensitive, time-critical nature of the data exchanged between the financial application and the mobile terminal; and
- the needs of customers and financial services companies for the highest levels of security and data integrity.

Degradations in wireless network performance can expose the financial service company's applications or data to unnecessary risk, since some performance degradations may appear to the applications network as security violations or attacks.

The wireless access network, for the applications detailed in Section II, should have a call blocking rate less than 1%, a call dropping rate less than 1%, a hand-over failure rate less than 1%, and a frame error rate of less than 1%.

Section IV. L. Service Quality Guidelines

The wireless network should have error-recovery mechanisms built in that enable it to recover from transient conditions that may result in lost or duplicate packets. The wireless network should have built-in techniques that enable it to overcome conditions that temporarily result in poor signal quality or wireless coverage limits.

The wireless network should similarly include technical methods of controlling interference, so that transmissions from multiple mobile terminals in the same area do not limit the transmission rate or the accuracy of signals and messages received by those terminals.

Service quality should be maintained by the wireless network even when mobile terminals approach and then enter hand-over from one transmitting base station to another.

Section IV. M. Support for Multicast and Broadcast Services

Certain financial applications imply rapid distribution of the same messages or alerts to large numbers of end users with a high level of simultaneity. In some cases, delivery of particular broadcast or multicast messages should be made to all end users on a broadcast or multicast address list within a specific number of minutes or seconds, independent of the locations of the end users on the list.

Rapid delivery of broadcast or multicast messages to their destinations implies that the wireless network should have the ability to maintain a broadcast or multicast address list, to edit or change such lists, to route messages quickly once the locations of the destination mobile terminals are known, and to recognize "time-to-live" specifications for each message. Of course, the wireless network should also be able to rapidly locate all the mobile destinations once a broadcast or multicast message is sent.

Rapid location of a large number of mobile terminals depends on a fairly regular flow of registration messages from mobile terminals to nearby location registers that typically forward “current location” information to a location register in the user’s or terminal’s home service area.

To enable rapid distribution of broadcast and multicast messages even to mobile terminals that are not in use, the network should have the ability to locate and activate a terminal that is not active and that may be in “sleep mode.”

The preceding paragraphs imply that financial applications offering broadcast or multicast message delivery to mobile terminals, with guarantees that all of the appropriate customer terminals are located and messages are delivered in a timely way, should be supported by mobile terminals that are “always-on.” These devices should always be partially powered at a level sufficient to enable them to exchange periodic registration messages with the local wireless network. This will allow the mobile terminals to be located and turned on by network commands when urgent broadcast, multicast or personalized alert messages are to be transmitted.

When a mobile terminal subscribing to a financial alerting service cannot be located by the wireless network operator’s mobility management system, the wireless network should notify the message originator that the application-level alert could not be delivered, so that the financial services company can take appropriate alternative action.

Section IV. N. Gateway Guidelines

Gateways are sometimes used in wireless information networks to perform filtering, formatting, terminal adaptation, encryption and other security functions. At least two types of gateways can be envisioned in connection with these networks:

- wireless gateways, which typically connect the wireless network to a data transport network, and which perform media conversions and user interface functions that format information for display on a mobile terminal or wireless handheld device; and
- middleware gateways, which typically support a presentation-level interface between client software running in the mobile terminal and financial services executing on the financial services company’s applications network.

The data streams transmitted for many mobile financial applications will employ industry-accepted strong encryption and authentication techniques end to end. Mobile financial applications data should not be decrypted at any intermediate points to reformat and adapt the data presentation to specific terminal designs, for that decryption could unnecessarily and unacceptably compromise highly confidential financial data.

In general, the factors noted in the previous paragraph suggest that format and media conversion functions, adaptation of mobile applications data to mobile terminal designs, and application-level authentication and authorization functions should be performed inside the financial services company’s firewall.

Section IV. O. Repair, Upgrade and Customer Service Guidelines

The wireless network operator will often be the provisioning agent for mobile terminals in its service territory. For such mobile terminals, some of which will be used for mobile financial applications, the

network operator will be responsible for arranging for repair and customer service of broken mobile terminals. The network operator should provide convenient methods, on a 24x7 basis, for customers to contact a service center and arrange for trouble diagnosis and repair of defective terminals.

The wireless network operator should also provide methods and tests for distinguishing defective mobile terminals from service quality and performance problems stemming from network problems, coverage holes, and interference and radio capacity limits. The network operator should track coverage- and network-related problems and should take steps to reduce their impact through steady improvements in base station placement and design, and through regular planned upgrades of wireless network capacity.

The wireless network operator should provide convenient methods for customers or financial services companies to contact a network service center to report potential or suspected wireless network problems for diagnosis and repair. Wireless network operators should establish standardized, precise and consistent error messages, and effective escalation procedures.

Section V. SOFTWARE SOLUTION GUIDELINES

This section summarizes guidelines for the system software, middleware and applications software that will be in terminal devices, in gateways and in servers supporting mobile financial applications and content for customers who access financial services with portable wireless personal digital assistants, wireless-enabled handheld and notebook computers, and advanced cell phones.

Much of the software for mobile financial services will support functions that are common across multiple applications in middleware. Examples of software that should be common across applications are modules that enable aggregation and presentation of information gathered from existing financial applications and modules that implement a financial services company's business rules and processes for the mobile/wireless environment, as illustrated in Figure 1. A major goal of financial services companies is to leverage existing middleware and messaging technologies (such as OFX/IFX and XML) for mobile financial services instead of building new middleware specifically tailored for mobile applications.

In general, this section addresses software at the application, presentation and session levels in the various computers and servers that may be used to implement the functional architecture shown in Figure 1. Software that is used in the various wireless network elements to operate base stations or other communications equipment is not addressed by these guidelines.

Section V. A. Mobile Applications Support Guidelines

The solution software modules or software platform provided to support mobile financial applications should be capable of supporting all of the business applications detailed in Section II with acceptable levels of usability, security and performance.

Since different financial services companies may implement different sets of applications and may change the applications supported or the way in which those applications are implemented, the mobile solution software platform and the modules that comprise it should be adaptable to the changing needs of financial services companies and their customers.

Solution software should enable financial services companies to offer different groups of financial applications to different end users. This capability would enable financial services companies to package applications in ways that support market segments with divergent needs, including but not limited to: mass-market consumers, private banking customers, financial services employees and other groups.

The solution software provided to support mobile financial applications should adapt to each financial services company's existing applications, internal networks and databases.

Section V. B. Service Quality Guidelines

Solution software for mobile financial applications should support extremely high concurrency, potentially involving thousands or tens of thousands of simultaneous users executing distinct applications and/or transactions, without appreciable degradation in usability, security, reliability, or

response time. The solution software architecture, and its implementation on multiple processors or servers, should therefore be highly scalable and reliable.

While most solution software will be independent of the underlying wireless network and will not need detailed adaptation to the wireless network, parts of the mobile solution software should be aware of the detailed characteristics of many mobile terminal devices so that financial services and data can be presented in an appropriate, usable way on each terminal's display.

To maintain transaction security and nonrepudiation, applications software and middleware may need to be cognizant of the types of wireless or wired channels over which financial services are being provided so that "rules" for appropriate service quality or behavior of the applications can be applied while financial transactions or applications are executed. These "rules" may, for example, embed reasonable assumptions concerning response times or error rates to help the application layer manage session initiations and terminations. The parameters describing normal wireless network operation will depend on the specific type of wireless network being used. Some built-in procedures for negotiating and managing service quality may be needed by the financial software platform so that high levels of resources are not devoted to transactions or applications that are unlikely to execute in reasonable time.

It is desirable for mobile solution software to be able to support differentiated services so that financial services companies can offer services at various quality levels to their customers, employees and business partners. It would be useful, for instance, for the solution software to enable financial services companies to offer applications to end users in multiple priority classes.

To support service quality and transaction/application flow, mobile solution software should implement a variety of timers that can be varied or engineered for specific applications and/or wireless channels. At minimum, mobile solution software should support programmable message timers, transaction or application timers, and session timers. These timers will be used by financial services companies and application providers to support transaction throughput, error recovery and session integrity over highly variable wireless transmission channels.

Section V. C. Compatibility with Wireless and Mobile Standards

The mobile financial software solution should be compatible with delivery of mobile financial services over a variety of wireless networks implemented in accord with widely accepted industry and international standards for wireless access, transport and mobility management. Wireless networks implemented in different parts of North America may be based on different versions of wireless standards. Since some financial services companies have very large regional or national footprints, it is important for the financial software solution to support implementation of mobile financial services simultaneously to customers using different wireless access standards and devices. For example, the software solution should support simultaneous use of any or all of the business applications listed in Section II over CDMA, GSM, TDMA (IS-136) and W-CDMA wireless networks.

One major implication of the preceding paragraph is that customers should be able to get seamless access to financial applications over the mobile networks of a large number of wireless carriers. The financial software platform should facilitate carrier- and technology-agnostic support for mobile financial services.

Section V. D. Wireless Devices Supported

The mobile financial software solution should support delivery of financial services to customers using a wide variety of mobile terminals or portable wireless devices. The services may not appear exactly the same on all terminal devices, and the mechanisms for message input or response may vary from one device to another. The mobile financial software platform is responsible for mediating these presentation-level device dependencies and tailoring the specifics of service delivery to particular devices so that the customer ends up with a highly usable, secure, reliable financial service as long as a mobile device that meets industry acceptable specifications is used.

Software in the mobile terminal used for financial services should allow customers to carry out multiple simultaneous activities, within limits imposed by each device's real-time processing capabilities and limits imposed to safeguard application- and data-level security. It would be useful, for example, to permit customers using mobile financial services to simultaneously use built-in calculators or "memo pads" in the middle of applications sessions.

Wireless software and terminal providers may want to design devices that can easily switch from one "mode" to another (e.g., from remote application mode to local computation mode) to enable useful implementations of multiple simultaneous activities. As an alternative, applications may be written to support a mid-session "pause" function that would allow a customer to carry out intermediate calculations or record a transaction summary while relevant session data are available. Some of these functions may be implemented in sufficiently powerful mobile devices, while other functions may entail network- or server-based implementations and use of cached session history in the form of recently used screens or forms data.

Wireless devices used for mobile financial services, and the underlying application software and middleware infrastructure, should support localized databases, making it easy for customers to store transaction records securely and in an appropriate abbreviated form after transaction or application sessions have ended. These records, which may be stored locally on the mobile device and which should also be stored by the financial services company in a way that can be easily accessed by the customer, would include definitive details of the application session or transaction required by applicable statutes and/or regulations: confirmation codes, transaction amounts, account numbers, payor and payee, etc. It should be possible for customers to access records of wireless transactions and application sessions over wired, as well as wireless, terminals.

Mobile solution middleware should be able to communicate the type of device that the customer is using as well as the user ID to financial application-layer software so that the financial services companies can restrict applications or data to devices that support security levels consistent with their security policies. The solution software should enable financial services companies to create rules, based on an abstract representation of the mobile device, that will let the financial services company's software determine "on the fly" which applications a given end-user mobile terminal device can access.

Section V. E. Software Usability

Software for mobile financial services is composed of several categories: applications software, service-enabling middleware and gateway or content adaptation software. The success of mobile financial services depends critically on the end-to-end usability of the applications. Software solution

providers consequently have critical responsibilities in designing and implementing software leading to usable, highly reliable, value-added applications.

Overall factors influencing the usability of mobile applications include typical time intervals for completion of application sessions or transactions, intelligibility and intuitiveness of user interfaces, ability of the software to adapt to varying terminal and network types, and predictability and stability. It should be possible for a typical user to complete many application sessions, for most of the application sessions described in Section II, in under one or two minutes, except when extensive browsing or data retrieval and processing are needed in back-end systems or middleware gateways. There is a category of complex transactions or application sessions for which end users do not mind longer sessions, but users should receive periodic progress indications during longer sessions so that they do not lose track of session status and abort active, but lengthy sessions.

Intelligibility and intuitiveness of the user interface pose critical challenges to software solution designers for mobile financial services, for the services should be supported on a large number of mobile terminal types with a wide range of user input and display capabilities. The software solutions should, furthermore, be capable of adapting to and supporting, modular add-on components (e.g., keyboards, alternative displays, additional memory). In general, applications should require a minimum number of keystrokes or keypad entries to execute commands and client server request/response exchanges, and to carry out local computations or message composition. Touch-sensitive menu keys or scroll wheels (or comparable input and navigation aids) on the mobile terminal should be exploited so that customers can quickly select applications or Web pages of interest and then choose an appropriate action. On the output side, software solution designers should adapt the presentation of information to the individual mobile terminal so that:

- the most important and relevant content is legibly rendered;
- the customer can clearly distinguish when additional information is needed for session completion; and
- the customer can easily get help with the application if needed.

To help financial services companies ensure that the vast majority of mobile applications and transactions are executed the way that customers intend, software solution designers should aim for software designs that implement applications in a predictable, consistent way despite variability of the wireless transmission channel and of the mobile devices used. This is not meant to imply that the time intervals, command streams or output displays are exactly the same from one terminal or wireless network to another, but there should be enough underlying uniformity so that the customer perceives a relatively consistent application environment and is not misled by variations in response times, input prompts or data presentation.

Section V. F. Security

The software solution offered to financial services companies for mobile financial services should support extremely high levels of security end to end, from the mobile terminal to the institution's back-end application network. Support for strong encryption and strong authentication will be needed.

The security solution should comply with recent specifications and guidelines of the BITS Security and Risk Assessment Steering Committee and the BITS Aggregation Services Working Group. In

particular, software supporting wireless financial services should comply with the authentication, authorization and application profiles contained in these documents.

In addition to supporting widely used encryption and authentication standards, the wireless solution provider should supply profile management software tools that will enable financial services companies to set up and modify, subject to appropriate security constraints, profiles for individual end users. The profiles so established by the financial services company for its customers may contain user-specific authentication and authorization data that will uniquely identify the customer, the specific financial applications he or she is entitled to execute, any restrictions on the way those applications can be executed, and the types of data each specific customer is entitled to view, to format (in connection with aggregation services, for example), or to execute transactions against.

The wireless solution provider should further supply profile management software that enables customers, within constraints or rules established by their financial services companies, to define or modify preferences for content formatting, message delivery and filtering of information.

Access to personal authentication or authorization information, and the ability to modify this information, should be protected and restricted to the highest possible appropriate level. The wireless software solution provider should supply financial services companies with secure logging and audit software to record the source and history of all requests for user profile creation or modification.

The end-to-end security architecture implemented in wireless solution software should support end-to-end transaction nonrepudiation. To accomplish this, the solution software should ensure that it can be proven who initiated a transaction or performed a specific activity, and what the transaction's completion status is. The information to prove who initiated or performed a specific activity, and the transaction's completion status, should exist at each transaction touch point.

The security architecture and its implementation in mobile solution software should allow the financial services company to offer differential levels of security and authentication based on transaction and application security requirements that may vary with the size of the transaction, the parties involved or information exchanged in the application session, or other factors.

Because the technology is not readily available to implement these guidelines, some financial services companies may choose to implement interim security solutions without end-to-end encryption to support initial offerings of mobile financial services. Approaches for near-term security solutions of this type should be based on risk assessment and technology availability. Furthermore, given the limitation of current technology, some end-to-end encryption options may actually pose a higher risk.

Since different financial services companies may make different security choices near-term, and since a number of these companies may want to offer differential levels of security and authentication, as described above, software solution providers may want to support a range of security architectures, including end-to-end encryption, in the middleware and application software that they offer. Software solution providers should provide effective transition strategies that will allow financial services companies to migrate from interim security approaches to end-to-end encryption where it is needed and becomes available.

Section V. G. Transaction Integrity

Wireless solution software should support industry-acceptable levels of transaction integrity for mobile application customers.

Wireless solution software should prevent duplicate transactions while dealing with factors specific to the wireless environment that may cause significant intra-session delays or session failures as customers move from areas with good wireless coverage to areas with limited or poor coverage. Records of incomplete or aborted transactions should be recorded by wireless transaction software to permit each financial services company to safeguard its financial integrity.

High frequencies of aborted transactions or repeated transaction attempts, for a specific customer, or within a specific area, may be associated with attempts to breach a financial services company's integrity or to compromise its transactions. Wireless solution software should provide capabilities that enable financial services companies to define or customize transaction rules whose violation would trigger security alerts or disabling of specific customer accounts or mobile devices for financial services.

Because the impairments or limits that are typical of wireless data services can cause transaction failures or requests for repeat transaction that may resemble violations of application security or transaction integrity, wireless solution software should maintain "reason codes" detailing the reason that particular transactions or mobile service sessions terminated. The "reason codes" should contain enough information so that the solution software can distinguish transaction failures stemming from imperfect wireless coverage from those caused by attempts to misuse or compromise the financial services company's applications or data.

Mobile solution software should support and enforce transaction integrity across financial services companies. Mobile terminals will be used for transactions or applications with several financial services companies, and a customer's transactions or financial data relating to one company should be protected and unavailable to other such companies if the customer carries out a series of transactions with several of them.

Section V. H. Session Management Guidelines

Wireless solution software should provide support for effective application session management over wireless channels in a way that maintains effective session security, auditability and integrity as a customer moves with a mobile device from one area of wireless coverage to another. It should be possible to execute one or more financial transactions, and to invoke one or more mobile applications, in the course of a single session.

Mobile session management should be done in a way that recognizes the limits of real-world wireless channels, which, because of network coverage and capacity limits, can cause signals to fade and connections to drop for short periods of time, in spite of the customer's interest in completing the application session or transaction. Session management features should be developed in ways that mitigate the impact of "dropped" sessions on existing applications.

Effective session management in a mobile or wireless environment may be based on protocols that support "session persistence" or session-reconnect features. These features would allow a particular customer using a particular device to automatically re-establish a session if wireless connectivity were

temporarily lost because of coverage holes, transient fading or wireless signals, or interference from other nearby wireless users.

Very high security should be maintained by whatever session-persistence or session-reconnect mechanisms are implemented, even if the customer is not required to go through a full authentication and authorization sequence to re-establish the session. Sessions should have unique names or identifiers, and end-to-end secure encryption should be maintained when sessions are re-established.

Application usability has additional implications for session management when persistent sessions are supported by the wireless software solution. In particular, when a session is re-established after a temporary interruption, the display and application state of the mobile terminal may need to be refreshed or resynchronized with the financial services company's application or server. This re-establishment of the display and application context should enable the customer to resume an application session or transaction where the session left off before interruption.

Session management software should enable the financial services company's servers or gateways to temporarily store session state, context and history for all sessions so that customers can resume transactions and application sessions easily after temporary interruptions stemming from transient loss of wireless coverage or connectivity.

It is desirable for mobile session management software to allow financial application sessions to be split across multiple terminals or delivery channels. It should be possible, for example, for a customer to start an application session on one mobile device and complete the session on another mobile device or on a wired personal computer.

Mobile solution software should support and enforce session and message integrity. Mobile solution software should protect the privacy and confidentiality of each customer's sessions and messages with each financial services company. The end-to-end security model implemented by mobile solution software should ensure this security and privacy, and should prevent unauthorized parties from injecting content or data into the customer's sessions and message flows.

Section V. I. Software and Operating Environment

Software solutions for mobile financial services should be standards-based and generally will consist of:

- application servers and wireless middleware (e.g., for security, directory and user interface functions) running behind the financial services company's firewall;
- content delivery servers for push and pull wireless applications;
- gateways to existing financial and account databases;
- content conversion software to adapt content to the design of specific devices,
- profile creation and management software; and
- application creation frameworks to enable financial services companies to write new applications and to modify existing wireless applications over time.

The end-to-end wireless software solution will also include "thin" or "thick" client software running in the end user's mobile device, allowing the mobile terminal to receive and process wHTML and XML content for display on the device, and allowing the mobile terminal to format its requests for secure transmission and secure transactions in ways that are compatible and interoperable with widely

available servers, gateways and databases. Thick client software running on the end user's device should be supported with over-the-air updates.

To promote stable, scalable environments for software development and execution that will have low life-cycle costs, wireless solution software should be developed using standards-based, object-oriented development environments (e.g. C, C++, Java). Servers, gateways, and solution middleware components should execute in real-time in UNIX, LINUX, or Windows NT operating systems. Wireless handheld or portable devices should utilize widely available operating systems and widely acceptable standards for transmission, information display and input, and browsing.

Software solution providers should supply application creation tools and rules with their software suites so that financial services companies can create and customize new mobile applications for end users in ways that do not compromise application interoperability, ease of use or security. Software solution providers should also supply application management tools and software with their software suites so that financial services companies can:

- enable or disable specific applications;
- measure and analyze application performance on a specific processor;
- measure and analyze end-to-end performance of specific mobile applications to specific mobile devices;
- perform software configuration management on individual servers and gateways; and
- maintain audit logs required by financial industry computing practices and by applicable banking and financial industry statutes and regulations.

Section V. J. System and Configuration Management Guidelines

Mobile solution software should follow industry-standard system and configuration management procedures for hardware and software. This guideline includes the use of standard protocols (e.g., SNMP), tools, and monitoring of critical conditions that will enable the financial services company to enforce resource limits and degrade operations safely and controllably in the event of module or system failures.

System and configuration management for the mobile financial services infrastructure should support remote monitoring of critical hardware and software so that financial services companies can achieve very high availability and reliable operation at controlled costs.

Section V. K. Privacy Guidelines

The wireless software solution should permit financial services companies to offer customers several levels of privacy in the handling of customer data, in accord with all relevant statutes allowing customers to restrict the use of personal information. The wireless solution software should enable financial services companies to record and enforce the privacy preferences of each customer so as to prevent the disclosure of a customer's transaction or financial histories, or aggregated financial data, to unauthorized businesses or individuals.

Section V. L. Customer Service Guidelines

The financial services company generally will be the customer for the software platform supporting mobile financial applications. Because financial services companies must satisfy the needs of large

numbers of consumers or other end users with extremely high reliability and dependability, and because those institutions operate with a variety of regulatory and due-diligence requirements, companies supplying software for mobile financial applications (or supplying individual modules of such software) should be prepared to provide the highest levels of customer support and immediate response to critical incidents.

Customer service should include predictive and diagnostic software to anticipate and isolate software problems, test software to stress code sequences, onsite support for responding to critical alarms and incidents, and service level agreements that guarantee specific industry-acceptable response time, availability, mean-time-to-fail, and mean-time-to-repair for the software platform and its components.

Section V. M. Support for End Users Outside Home Areas

It is important for customers who subscribe to mobile financial services to be able to gain access to and use mobile applications outside of the “home areas” to which they are assigned by their wireless network operators. Two types of support for users outside of their home areas are needed:

- A customer should be able to use mobile financial services outside the home area in other locations served by the same wireless network operator.
- A customer should also be able to gain access to and use mobile applications in places served by other wireless carriers, but which are not served directly by the customer’s normal wireless carrier.

To promote the access to wireless financial applications implied by these guidelines, wireless server, gateway and middleware software solutions should be able to support financial services that are transported by multiple wireless network carriers using a variety of wireless transport technologies and standards. This means that wireless software solutions should have the ability to adapt to and interoperate over communications channels of various bandwidths and transmission formats without significant impairments or changes in usability other than variations in transmission delay that may be entailed by channels of different bandwidths or by networks engineered for different throughputs or capacities.

Wireless access from outside the customer’s home area may involve extra delays for registration and authentication on the wireless network from the visited, or “foreign,” area. Mobile financial applications and associated server, gateway and middleware software should be able to adapt to these extra delays that may be encountered when the mobile application is invoked or, mid-session, as the mobile customer encounters hand-offs from one area or network to another.

Section V. N. Transparent, Seamless Services

Solution software providers should promote ease of use for mobile applications by ensuring that customers can get access to and execute applications with essentially the same control sequences or commands from one geographic area to another, and from one mobile network operator’s network to another. Thus, a customer using the same mobile device to access wireless financial services should be able to use those services with the same input commands, regardless of the customer’s location and independent of the specific wireless carrier whose mobile data services are being used.

Application performance, and thus customers’ application experience, may vary from one mobile network to another because of differences in the carrier’s engineering or the bandwidths of the

services each carrier offers. However, the commands, messages and responses accepted by solution middleware, server and gateway software, and application software should be essentially independent of the specific wireless data services the customer is using for access to the financial services company's network.

Solution software should also, to the extent possible, promote ease of use for mobile applications by ensuring that the control sequences or commands used to access and execute mobile financial applications are similar from one mobile device to another. Because mobile devices are highly variable in their displays and user interfaces, it may not be possible for mobile software solution providers to design applications that use exactly the same control sequences from one device to another. Providers of application development platforms should, nonetheless, offer application creation environments that allow financial services companies to construct similar names and command sequences and the mobile devices it is targeting for a major fraction of its target market.

As described above, it should be possible for a financial services company, or application developers working on its behalf, to implement a given application with commands and control sequences that use similar command names and sequences on a wide variety of mobile terminals. Solution providers should aim to support this level of application transparency even if the target set of mobile terminals use very different display formats and even if they employ differing input techniques, e.g., full keyboard input, drop-down menu selections, radio buttons or check boxes.

Finally, mobile solution software should support and be compatible with transparent, seamless transfers, or hand-overs, between different wireless carriers and networks. Mobile financial applications and middleware should operate in a transparent way for mid-session hand-overs from one network or carrier to another, even when the wireless networks involved in the hand-over are able to offer different bandwidths or throughputs to the applications.

Section V. O. Software Performance Guidelines

Wireless solution software, when implemented on readily available high-performance, highly scalable computing platforms, should be able to support a very large number of concurrent transactions or application sessions for multiple users and multiple mobile devices without sacrificing performance, security or usability. "A very large number," in the context of scalability, may be between tens of thousands and millions.

The software solution should be compatible with and facilitate load balancing among critical system components so that financial services companies can engineer their application networks for predictable, controllable performance and graceful degradation under overload or failure conditions.

Mobile software solution providers should have plans for disaster recovery that will enable financial services companies to quickly restore operations when they are affected by natural disasters. The recovery plans should include code escrows and backup procedures for customer data, applications and critical system configuration and management data.

Section V. P. Support for Multicast and Broadcast Services

Some of the applications detailed in Section II imply delivery of the same content to multiple customers. Examples of such applications include delivery of advertising or "push" promotion cross-

selling, news updates and certain classes of alert messages. Some applications involving delivery of the same content to multiple customers do not have specific delay, simultaneity or delivery confirmation requirements. Other applications in which the same content is delivered to multiple customers may have stringent timing, delivery confirmation or alternate message delivery requirements in the event that delivery of the original content cannot be confirmed within prescribed intervals.

In view of the range of message and content delivery specifications noted above, wireless software solutions should provide financial services companies with several capabilities supporting multicast and broadcast services that can be flexibly applied by financial services companies in tailoring applications to specific customer or end user needs:

- Financial services companies should be able to use wireless solution software to create, administer, and manage broadcast or multicast address lists.
- Wireless solution software should enable customers to add themselves, after appropriate authentication and authorization, to broadcast and multicast address lists.
- Wireless solution software should enable customers to delete themselves, after appropriate authentication and authorization, from broadcast and multicast address lists.
- Wireless solution software should enable the financial services company to record whether a particular application has maximum delay requirements for message delivery.
- The wireless solution software should enable the financial services company to record message delivery times and track message delivery intervals to establish whether maximum delay requirements are being met.
- Wireless solution software should enable customers to specify arrangements for alternate message delivery in the event that delivery of certain high-priority messages (e.g., personalized alerts) cannot be confirmed within agreed-upon time intervals. These arrangements for alternate message delivery may involve message delivery to another wireless device, email or voice mail.

Section V. Q. Gateway Guidelines

Gateways are used in wireless information networks to perform filtering, formatting, terminal adaptation, encryption and other security functions. Two types of gateways can be envisioned in connection with mobile financial applications (similarly defined for Networks, Section IV. N):

- wireless gateways, which typically connect the wireless network to a data transport network, and which perform media conversions and user interface functions that format information for display on a mobile terminal or wireless handheld device; and
- middleware gateways, which typically support a presentation-level interface between client software running in the mobile terminal and financial services executing on the financial services company's applications network.

In general, as noted above, format and media conversion functions, adaptation of mobile applications data to mobile terminal designs, and application-level authentication and authorization functions should be performed inside the financial services company's firewall.

Both types of gateways described above should adhere to the security guidelines outlined in Section V. F., the transaction integrity guidelines outlined in Section V. G. and the software and operating environment guidelines outlined in Section V. I.

Gateways should support or be compatible with authentication, authorization and confidentiality at the client level, and should support transaction, session and application security across mobile applications and the financial services company's application servers and existing backend network.

Section V. R. Operational Database Guidelines

Wireless solution providers should provide the operational databases that would enable a financial services company to establish, administer and maintain mobile financial services for large numbers of customers. Among the databases and database software that should be provided are:

- a database to record technical and operating characteristics of mobile devices;
- a database to record technical and operating characteristics of wireless networks and services that can support the mobile financial applications that are offered;
- a customer or end-user database recording customer personal information, applications that each customer is authorized to use, billing arrangements, default device, application preferences, alternate message delivery instructions and security information;
- a session database tracking all active sessions, along with a list of active devices, users and applications;
- application, session and transaction logs for audit purposes; and
- an authentication database containing up-to-date passwords or unique identifying information for each customer.

Section V. S. Repair, Upgrade and Customer Service Guidelines

Wireless solution providers should provide testing and diagnostic tools that will enable financial services companies or their application providers to identify and localize software failures and limit their impact on the security, safety and integrity of mobile financial services. Software or hardware components that are highly shared—processing very high volumes of concurrent transactions—may imply comparable high levels of redundancy or backup to achieve reliability and availability levels necessitated by the financial services company's underlying fiduciary, due diligence and regulatory responsibilities.

Wireless software solution vendors should enable financial services companies to meet very stringent levels of reliability, availability and security by implementing software repair and upgrade techniques that can be activated in real time and from remote locations, preferably without disrupting or adversely affecting application or transaction execution on redundant servers or databases.

Financial services companies should be able to choose from several levels of customer service for diagnosis and repair of software, server or gateway faults. Since mobile end users are not limited to transaction execution during regular business hours, software solution providers should offer at least one level of service that ensures timely diagnosis and repair on weekends, evenings and holidays, and at other times outside of normal business hours.

Mobile solution software vendors should support a “warm hand-off” of end-user service or support requests that may be directed to financial services companies. The “warm hand-off” will let financial services companies refer end-user inquiries quickly and efficiently to the proper level of customer support in the solution provider's organization. Since end users will want access to and help with mobile financial services at practically any hour, software vendors should implement a customer support approach with 24X7 availability.

Section VI. HANDHELD DEVICE/MOBILE TERMINAL GUIDELINES

This section summarizes guidelines for handheld devices, mobile terminals and portable computers with wireless connectivity that will be used to access and execute mobile financial services.

Section VI. A. Mobile Applications Support Guidelines

It should be possible for end users, after appropriate authentication and authorization, to access any or all of the mobile financial applications described in Section II on Mobile Application Business Guidelines. Different financial services companies may offer different packages of mobile financial applications, and various end-user populations may select or predominantly use different combinations of the business applications listed in Section II.

Section VI. B. Mobile Terminal Usability

For the mass market, it is expected that mobile financial services will be supported by mobile terminals and wireless portable devices that are generic in nature, rather than by terminals or devices that are specifically designed for mobile financial services. Specialized user populations, such as specific work groups in the financial services industry, may use wireless terminals that are specially designed or optimized for specific applications.

Usability of mobile financial applications is paramount. End users should be able to easily and reliably gain access to and use financial information for personal and business decisions and actions. In general, the full set of mobile financial services outlined in Section II can be supported on a terminal or portable device that supports a graphical user interface with simple input (e.g., through a pointing device or buttons) and a high-contrast display that can render graphics and limited text legibly even in daylight conditions.

Recognizing that different financial services companies may choose to implement the presentation of mobile financial services in different ways—for example, with different combinations of text, graphics and input commands for display and input of information—the provider of the mobile terminal or wireless handheld device should be prepared to meet the guidelines of each financial services company for usability and clarity of information presented on the terminal's display. In general, the mobile terminal or wireless handheld device should be able to receive messages relating to mobile financial applications and display them appropriately for the end user. The mobile terminal should also enable the end user to input messages or responses to messages in a way that is convenient and reliable. Mobile terminal input and display interfaces should be consistent with the financial services industry's acceptable standards for usability and legibility.

Larger display areas and longer battery lifetimes generally will promote usability for mobile terminals and for the applications. Rated battery life in excess of one week, with the mobile device in fairly steady use, will permit many users to complete short business trips without the need for recharging. Since it is essential for financial services customers to reliably distinguish small features (e.g., numerals, currency units, decimal points) on a small screen, terminals used for mobile applications should have excellent screen lighting, high contrast and high resolution.

Limited sets of mobile financial services may be implemented on terminals or handheld devices with voice interfaces rather than graphical displays. Examples of such implementations include mobile financial services that are activated by customers using cell phones to communicate with interactive voice response (IVR) systems.

Section VI. C. Compatibility with Wireless and Mobile Standards

The mobile terminals and handheld devices used for mobile financial services should support widely available standard interfaces for mobile data services so that customers can use mobile financial services from a wide variety of indoor and outdoor locations. The wireless, or radio, interfaces supported by these devices should be based on publicly defined standards rather than on proprietary or closed wireless interfaces.

In addition, the mobile terminals and wireless handheld/portable devices should support publicly available and widely deployed mobile applications protocols for mobility management so that customers can access mobile financial applications outside of their home service areas and while they are in motion within a particular wireless network or moving from one network operator's service territory to another's.

While the financial services industry has a preference for mobile terminals that support public, standard interfaces and protocols, it is possible that some financial applications could be supported over ubiquitously deployed, widely available networks that use private or proprietary networks. When proprietary networks or interfaces are used, it is important that the mobile terminal and the wireless network still meet the minimum usability, security, interoperability and reliability/maintainability needs of the financial services industry for mobile financial services.

Over the long term, mobile terminals used for financial applications should support or be compatible with indoor wireless networking standards, including, but not limited to, the IEEE 802.11 family of specifications in addition to supporting public wide-area wireless standards such as GSM, IS-95, cdma2000 and W-CDMA (UMTS). Support for or compatibility with indoor wireless LAN standards may be achieved through auxiliary devices such as PC cards or wireless modems.

In addition to built-in support for wireless local area network standards, future mobile terminals should provide for "piconet," or personal area network, interfaces, at least to the extent that personal area network standards offer local communications advantages that significantly complement or surpass the device's built-in wireless LAN capabilities. Bluetooth and IrDA are examples of two personal area network interfaces that may expedite stored-value point-of-sale transactions.

While it is not the intent of the financial services industry to preclude combinations of devices (e.g., terminals, memory, modems or power sources) for mobile financial services, multiple pieces of equipment are at best a temporary, inconvenient way to access mobile applications. In most cases, large-scale mobile financial applications should be supported by portable terminals that include sufficient display, input, memory and wireless modem capabilities to allow an end user to access and effectively use the range of financial applications noted in Section II.

Section VI. D. Mobile Terminal/Wireless Handheld Device Software Guidelines

Several types of software will run in mobile terminals and wireless devices used for mobile financial applications: an operating system of some type; browser or display interface software; device drivers of various types; middleware implementing common functions needed by multiple applications; and application software modules.

The mobile device's operating system should have the ability to run multiple financial applications, some concurrently, and should make stored data available to multiple applications in a way that is consistent with security of the applications and the data. The operating system, together with any device or network middleware supporting security guidelines for mobile financial applications, should effectively support the financial services company's security practices by permitting applications to reserve memory and protect from intrusions when they are running. The operating system and security middleware should also protect data being used by applications from use by unauthorized or nonsecure applications. Thus, mobile terminal/wireless device software should support security for applications, for the memory that applications use when they are executing, and for the data that the applications use and generate as they execute.

Mobile terminals for financial services can include industry-standard browsers, messaging and display software that support highly usable, secure, reliable transactions and financial applications and that adhere to the other guidelines outlined in this document.

Browser, messaging and display interface software should support strong encryption and strong authentication so that the mobile terminal provides appropriate security and safeguards against unauthorized use. The browser should be easy to use for mobile financial services, supporting base-level wireless markup language (WML) and interoperability with any base-level WML implementation. Over time, it is expected that mobile terminals and associated system software will be further enhanced to include, among other components, a Java Virtual Machine (JVM), providing a common display and code execution environment, so that financial applications can run on many types of devices with minimal change or adaptation from device to device. This will limit life-cycle development expenses for mobile financial applications software.

In some circumstances, the manufacturer of mobile devices or the wireless network operator who provides such devices for end users may want to upgrade the operating system or other system software or middleware after the device has been given to the end user. While it is technically possible to download such software to the mobile terminal over wireless communications channels or through standard wired connections to desktop computers or local area networks, financial services companies will need to evaluate the security of such software before it is downloaded to already provisioned devices. Manufacturers of mobile devices and mobile network operators should take steps to ensure that all operating system software and middleware, whether the original versions provided with the devices or subsequent upgrades, meet industry-acceptable specifications of financial services companies for security. To comply with these industry-acceptable practices, all system and application code should have signatures to validate their authenticity and integrity.

Section VI. E. Mobile Terminal Security Guidelines

The mobile terminal/wireless handheld device should support the end-to-end security model implemented by the financial services company to safeguard the privacy and integrity of customer and transaction data. The device should support strong end-to-end encryption and strong authentication

procedures that will give subscribers access to the minimum data and applications they are authorized to use for each mobile financial application.

Each mobile terminal or wireless device in use for mobile financial services should have a unique equipment identifier that will be used in gaining access to the wireless channels and carrier services that will be used to transport mobile financial applications. The unique equipment identifier should be transmitted by the mobile terminal/wireless device to the wireless network in the area that is instantaneously occupied by the mobile terminal or wireless device. This information should be used to authenticate the end user's equipment and authorize the use of specific wireless services in that area.

The mobile terminal should have the capability to lock until a unique, correct password (or an equivalent unique identifier) is input by the end user. The password or other unique identifier should conform to generally accepted industry standards (e.g., FIPS 140 Level 2). These industry standards or specifications should support authentication and tamper-resistance for the mobile terminal that conforms to financial services companies' needs. This first-level password should be requested after the device is turned on but before its wireless capabilities can be used for communications over local or wide area wireless networks.

The mobile terminal should have the ability to encrypt some information and make it inaccessible, even after the first-level password or identifier is supplied, so that highly confidential information can be stored in the device without risk of immediate disclosure or discovery if the device is left unattended. Access to this encrypted information should be provided only after successful entry of another password or unique identifier meeting generally accepted industry standards. The mobile terminal should support multiple user accounts on the same device in a secure way. In general, the mobile terminal should support multiple first-level passwords or unique identifiers for authentication of multiple users. In addition, the confidential or private data stored on the device by each user should be protected from disclosure to other users who are authorized to use the same device. Thus, the mobile terminal should support multiple second-level passwords or unique identifiers. The mobile device should not capture transaction logs.

When the mobile terminal's stored data is synchronized with the contents of a desktop computer or other data storage system, the synchronization should be performed only for the authorized, authenticated user who initiated the synchronization. Thus, data and other information are synchronized on the mobile terminal for a single user at a time.

Because the technology is not readily available to implement these guidelines, some financial services companies may choose to implement interim security solutions without end-to-end encryption to support initial offerings of mobile financial services. Approaches for near-term security solutions of this type should be based on risk assessment and technology availability. Furthermore, given the limitation of current technology, some end-to-end encryption options may actually pose a higher risk.

Since different financial services companies may make different security choices near-term, and since a number of these companies may want to offer differential levels of security and authentication, providers of handheld wireless devices, mobile terminals and portable computers that are used for mobile financial services should support a range of security architectures, including end-to-end encryption and strong authentication, in the middleware and application software that they rely on. Manufacturers or providers of these mobile terminals and handheld wireless devices should provide

effective transition strategies that will allow financial services companies to migrate easily from interim security approaches to end-to-end encryption and strong authentication where it is needed and becomes available. The effective transition strategies for migration to end-to-end encryption and strong authentication should include convenient, secure methods to upgrade the security mechanisms used by a particular mobile terminal that does not require the owner or user of that device to deliver it to a remote service location for the necessary upgrade.

Section VI. F. Repair, Upgrade and Customer Service Guidelines

Since the mobile terminals used for mobile financial services will, in general, be generic devices used for several types of mobile communications and not just for financial applications, it is expected that customers will obtain the mobile terminals through normal distribution channels. For the mass market, these distribution channels will be through wireless network operators or through mobile terminal manufacturers. For a specific company's mobile workforce, the company's information technology department may select and certify certain types of devices for company use and may make arrangements with network carriers and/or device manufacturers and distributors to provide the mobile devices to employees.

The financial services company, based on the description above, is not involved in the direct provisioning of mobile terminals and therefore is not directly responsible for repair, upgrades or customer service for mobile terminals or for the wireless carrier services used by mobile financial applications. The network operator and/or mobile terminal manufacturers should provide over-the-air provisioning, updating, monitoring and diagnosis for the mobile terminals.

Financial services companies do, however, have some interest in ensuring minimum levels of reliability and responsiveness in the diagnosis of problems and servicing of mobile devices and wireless carrier services, even if those financial services companies do not assume liability or responsibility for repair and servicing of malfunctioning portable wireless devices.

In general, the provisioning agent for the wireless device—the entity that supplies the device to the customer—is expected to provide at least two levels of customer support and servicing. Level 1 customer support will encompass initial customer contact, trouble diagnosis and repair. Level 2 customer support will encompass trouble diagnosis and repair for problems that are resistant to rapid diagnosis and repair.

The manufacturer of the mobile terminal should supply test scripts and written procedures to provisioning agents to enable trouble localization to be performed, thus enabling the provisioning agent or the customer service agent to distinguish problems with wireless device hardware, wireless device system software, wireless device applications software and the wireless network.

In the course of repair of a mobile terminal, the privacy and integrity of any and all user data stored on the mobile device should be maintained by the entity carrying out the repair. If the device supports multiple users, the privacy and integrity of data stored for all users should be maintained during the repair process, and the security mechanisms implementing separate authentication by end users before they get access to their own private data should also be maintained during the repair process.

Section VII. CONCLUSIONS

In order for mobile financial services to be viable in the marketplace, cooperation among the industry segments supporting end-to-end guidelines for mobile services is essential. The *BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines* seek to encourage that cooperation in order to create innovative, high-quality, secure and easy-to-use mobile applications. The guidelines are intended to foster discussion within the industry, and a common understanding of technical and business practice to expedite implementation of mobile applications.

At the time of this writing, serious concerns are being raised about the security of wireless networks. Organizations are using WLANs despite immature technology and inadequate security in both handheld devices and the current WLAN standard, 802.11b. Common risks associated with these problems include financial loss from unauthorized transactions, disclosure of sensitive proprietary information, intrusion into the network and service disruptions. The guidelines are an attempt by the industry to establish requirements that will mitigate these security risks.

The result of an interactive, informed process, the guidelines have been thoroughly vetted by BITS and Roundtable member institutions, as well as those in the vendor community. Those companies that meet these challenges will help to accelerate the development of high-quality mobile products and services, and broaden customer acceptance of these technologies.

APPENDIX

Mobile Financial Services Working Group Co-Chairs

Kathy DeWit, Wells Fargo & Company, and Sam Phillips, Bank of America Corporation

PARTICIPATING INSTITUTIONS

724 Solutions, Inc.*
ABN-AMRO North America, Inc.
Air2Web*
American Banker
American Banker Association (ABA)
AmSouth Bancorporation
AT&T Wireless Services
Baltimore Technologies, Ltd.
Bank of America Corporation
Bank of Montreal
BANK ONE CORPORATION
BB&T Corporation
BitFlash, Inc.
Capital One Financial Corporation
Charles Schwab Corporation, The
Citigroup Inc.
CMG Telecommunications*
Comerica Incorporated
Commerce Bancshares, Inc.
Compaq
Credit Suisse First Boston
Cullen/Frost Bankers, Inc.
CUNA
Curious Networks
Diversinet*
Everypath*
FDIC
Federal Reserve Bank of Chicago
Federal Reserve Bank of New York
Federal Reserve Bank of Richmond
Federal Reserve Board
Fidelity Investments
FleetBoston Financial Corporation
Foley Hoag, LLP
Fortis, Inc./Assurant Group
FSTC
Heller Ehrman
Hewlett Packard
Hitachi Research Institute
HSBC USA, Inc.
Huntington Bancshares Incorporated
IBJ Whitehall Financial Group
IBM Wireless solutions
Independent Community
Bankers of America (ICBA)
J.P. Morgan Chase & Co.
KeyCorp
Kinexus
KPMG
Kyocera Wireless Corp.*
LegalNet Works, Inc.
M&T Bank Corporation
MBNA Corporation
Marshall & Ilsley Corporation
Mellon Financial Corporation
Mercantile Bankshares Corporation
Metavante Corporation
MIST Inc.*
MOBILEUM*
NAIC
National City Corporation
National Communications Systems
Nationwide
Neomar
Nextel*
Nextenso*
Nokia
Northern Trust Corporation
NTT DoCoMo USA, Inc.
Office of Science and Technology Policy
Openwave Systems, Inc.
Palm, Inc.
PCIA
PNC Financial Services Group, The
Pricewaterhouse Coopers, LLP
Prudential Insurance Company of America

Qualcomm Internet Service
Raymond James Financial, Inc.
Regions Financial Corp.
RSA Security*
Spectrum EBP, LLC
Sprint PCS
State Farm Mutual Insurance Companies
Sun Microsystems
Sun Trust Banks, Inc.
SynchroLogic*
Synovus Financial Corporation
Telcordia Technologies
U.S. Bancorp
U.S. Department of the Navy

USAA
Veridian Corporation
VeriSign, Inc.*
Verizon Wireless
VISA USA
Wachovia Corporation
Washington CORE
Washington Mutual, Inc.
Wells Fargo & Company
Whitney Holding Corporation
William Barr Consulting, LLC
w-Technologies*
Yahoo! Inc.
Yodlee, Inc.*

* Request for Information Respondents.

Phase I BITS Staff: Alice Cho, Teresa Lindsey, Tanya Bailey

Phase II BITS Staff: Jennifer Dickerson, Iris Simpson, Susanna Space



MEMBER INSTITUTIONS

ABN AMRO North America, Inc.
AEGON USA, Inc.
Allfirst Financial, Inc.
AMCORE Financial, Inc.
American General
AmSouth Bancorporation
Aon Corporation
Associated Banc-Corp
BancorpSouth, Inc.
BancWest Corporation
Bank of America Corporation
Bank of New York Company, Inc., The
Bank of Tokyo-Mitsubishi Trust Company
BANK ONE CORPORATION
BB&T Corporation
Capital One Financial Corporation
Charles Schwab Corporation, The
Charter One Financial, Inc.
Chubb Corporation, The
Citigroup Inc.
Citizens Financial Group, Inc.
City National Corporation
Comerica Incorporated
Commerce Bancshares, Inc.
Compass Bancshares, Inc.
Countrywide Credit Industries
Credit Suisse First Boston
Cullen/Frost Bankers, Inc.
Edward Jones Investments
F.N.B. Corporation
Fidelity Investments
Fifth Third Bancorp
First Commonwealth Financial Corporation
First National of Nebraska
First Tennessee National Corporation
Provident Financial Group, Inc.
First Virginia Banks, Inc.
FleetBoston Financial Corporation
Ford Financial
Fortis, Inc./Assurant Group
Fulton Financial Corporation
General Motors Acceptance Corporation
Goldman Sachs Group, Inc.
Guaranty Financial Services
Harris Bankcorp, Inc.
Hartford Financial Services Group, Inc., The
Hibernia Corporation
Household International, Inc.
HSBC USA, Inc.
Hudson United Bancorp
Huntington Bancshares Incorporated
IBJ Whitehall Financial Group
ING Americas
Jefferson-Pilot Corporation
J.P. Morgan Chase & Co.
KeyCorp
Legg Mason, Inc.
M&T Bank Corporation
Marshall & Ilsley Corporation
MassMutual Financial Group
MBNA Corporation
Mellon Financial Corporation
Mercantile Bankshares Corporation
National City Corporation
National Commerce Financial Corporation
Nationwide
Northern Trust Corporation
Old National Bancorp
Pacific Century Financial Corporation
PNC Financial Services Group, The
Provident Bankshares Corporation
Providian Financial Corporation

Prudential Insurance Company of America
Raymond James Financial, Inc.
RBC Centura Banks, Inc.
Regions Financial Corp.
Riggs National Corporation
Sky Financial Group, Inc.
State Farm Insurance Companies
SunTrust Banks, Inc.
Synovus Financial Corp.
TCF Financial Corporation

Union Planters Corporation
U.S. Bancorp
United Bankshares, Inc.
USAA
Wachovia Corporation
Washington Mutual, Inc.
Wells Fargo & Company
Whitney Holding Corporation
Zions Bancorporation
Zurich North America