

The Future of Wireless Banking

Implementation of Wireless Banking and Financial Systems

Rod Ghani
Senior Consultant
IBM Global Services
03/15/2001

Introduction

Have you seen change yet?

Today's banking and trading institutions realize they must move and move quickly to capitalize on new business opportunities in wireless banking and trading. Resistance to the implementation of wireless banking can lead to major losses at the business and market share levels.

Wireless service soon will be a necessity for the end-user. Although many technological barriers need to be overcome, it is imperative to embrace the change.

Wireless banking and trading is only an extension of the product offerings for the financial institutions. It is not an extension of web technology, as often perceived.

Online banking and online trading works from standard TCP/IP connection to the Internet using a PC, while wireless applications present a much greater challenge.

Today, wireless banking lacks leadership in enforcing one standard. There are several network standards, PDA standards, browsing standards, protocol standards...etc.

In the wireless world, airwaves are the only vehicle to send and receive data. Depending on the physical location- inside or outside of a building, near or far from a tower, in a small town versus a metropolitan area- quality is highly variable.

Did my order go through?

Non-repudiation is one of the most contesting issues in wireless banking and trading. The user needs to have proof that the transaction has been executed and confirmed.

Wireless banking is revolutionizing the makeup of every financial and banking institution. It is radically transforming the services, needs, and expectations of societies across continents, regardless of culture. In the next twenty-four months and beyond, massive changes will occur in the way we interact with banks and trading institutions regarding our business and personal finances.

The revolution is driven by the client (end-user) demanding to have the information available conveniently anytime, anywhere. Immediate access is expected and required.

Change at the institutional level is not an easy task. Adaptability and flexibility are needed when dealing with a variety of legacy systems, connectivity issues, protocol challenges, and a constant explosion on the market of new devices. Large institutions are handicapped by their size and have to become aggressive to keep up with the rapid times.

Today, B2B, B2C, B2G and B2E are recognized to be vertical online markets. Wireless is going to subdivide these markets, and new services will emerge targeting new user groups.

Data managers and system developers are expected to offer more effective and efficient methods in data delivery, anytime, anywhere, using any device, regardless of platform, protocol, browser, service provider, financial institution, etc.

A snap shot of the future

- The Gomez Research estimates that the number of people accessing personal account information online will grow from approximately 8 million in 1998 to nearly 40 million people in 2003. Given the numbers, banks and other financial providers must realize the opportunity inherent within Internet and wireless capabilities.
- According to Jupiter Communications, approximately 100 million people in the U.S. will have wireless non-PC web access by the year 2003, versus 155 million landline access from PCs. This deduces that non-PC access will grow to 65% of the wireline PC access market within the next three to four years.
- According to Forrester research, almost 120 million Europeans already use mobile phones, exchanging more than two billion wireless text messages each month.
- By 2003, Forrester projects 219 million Europeans, or one-third of the population, will be on the wireless bandwagon. Of the 50 European e-commerce executives interviewed by Forrester, 90 percent plan to launch sites that will be accessible by mobile phones
- Financial products and services provide an ideal setting for Internet delivery. M-Bank is well positioned to serve this industry with companies such as Wells Fargo and Co. (NYSE:WFC), Bank of America Corp. (NYSE:BAC), Providian Financial Corp. (NYSE:PVN), MBNA Corp (NYSE:KRB), and Capital One Financial Corp. (NYSE:COF).
- A major bank reports that over 3 million online banking customers, representing more than 20% of its checking account customer base that it continues to sign up approximately 130,000 new online banking customers a month. Also, more than 750,000 online banking customers have signed up for the bank's electronic billing and payment service, says the institution, and the total dollar value of payments processed grew 36% last year. Over 3.1 million EBPP were made, totaling more than \$1 billion.
- "It took us over 10 years to reach two million online banking customers and only nine months to add one million more," says Jeanine Brown, Interactive Banking executive.
- GartnerGroup predicts that by 2004, 80 percent of new applications for consumer use will permit access from mobile device clients (Source: GartnerGroup conference 1999).
- GartnerGroup research estimates there are more than 60 million employees worldwide working outside the traditional office setting. The Gartner study also says that the number will grow to 108 million by 2002.

Users Interest in Phones with E-Mail		
	Current Users	Potential Users
Definitely Interested	8.3%	13%
Probably Interested	8.0%	13%
Maybe Interested	13.3%	23%
Probably Not Interested	25%	26%
Definitely Not Interested	45%	25%
Source: The Strategis Group		

Little G History

1G is the first generation in mobile technology. Started in the late 1970s until the late 1980s.

2G began in the 1990s and it is still being used today, such as CDPD, CDMA, and GSM.

3G is the third-generation of wireless. It is expected to reach maturity between the years 2003 and 2005.

3G is expected to deliver enhanced voice and data and even video. Its bandwidth can be as high as 2 Mbps and will operate at 2 GHz.

Will Wireless banking play a major role in new markets?

P2P (Person to Person), and P2A (Person to Anyone) will play a major role in the financial world. We will witness an abundant in money transfers. A user can make a payment, have it automatically deducted from the appropriate account, and deposited into the recipient account, with an email acknowledgement.

It's about time

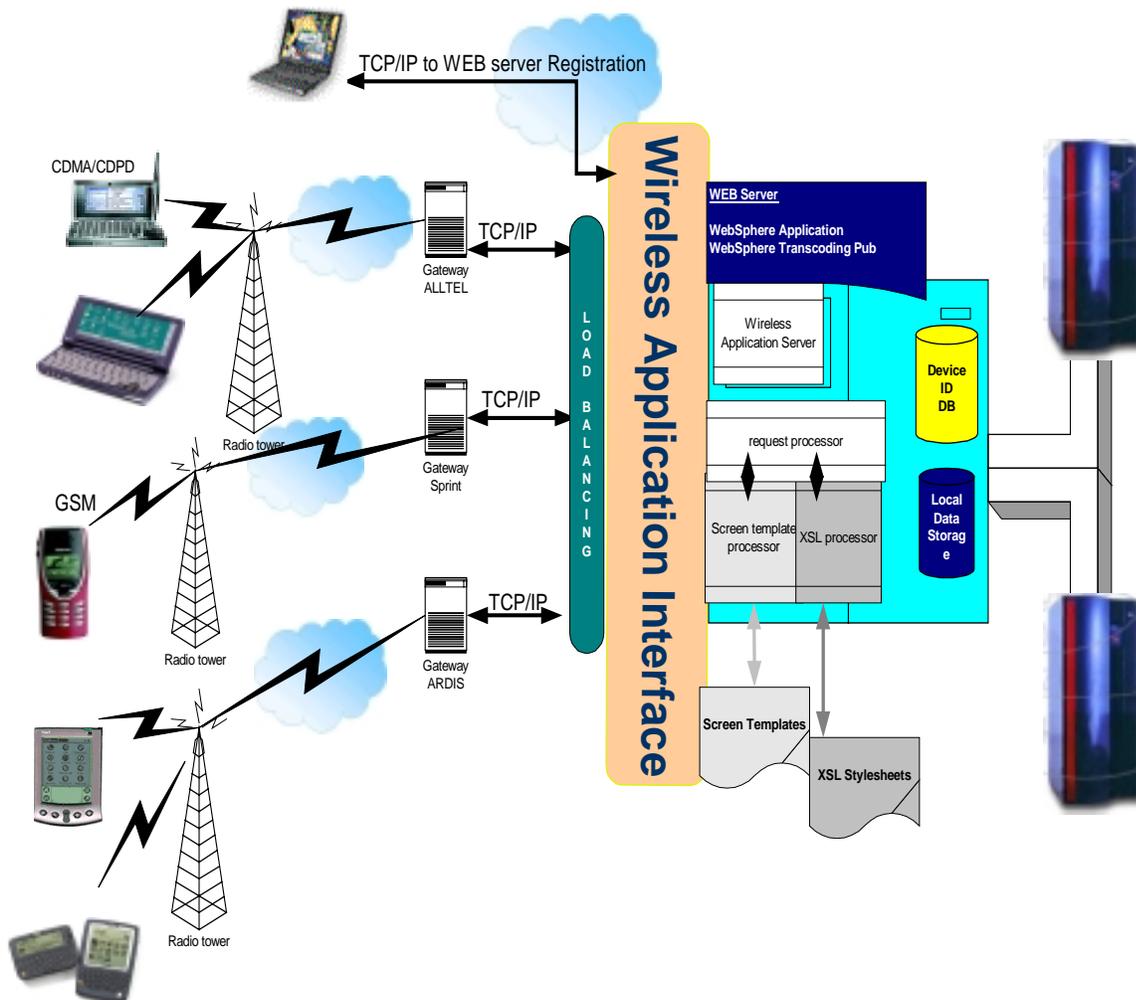
Time is the essence. Wireless banking and trading advantages are increasing by the day due to a rapid advancement in technology, rapid growth in wireless coverage, cost reduction in networking, and improvement in handheld devices, and bandwidth efficiency. Today, we can accomplish far more in wireless services, where it was not cost justifiable a year ago. With that in mind, WSP (Wireless Service Providers), corporations, and financial institutions can bank on the growth and take advantage of these opportunities.

The winners in today's wireless world are those who keep up with the change, cope with the challenges, and utilize the products and services offered.

Financial institutions must drive to enhance the systems delivery to create layers of an open system environment. Those who will use standard protocols will expand and thrive. Successful wireless implementation is delivered when the end-user can interact with the data easily, securely, and independent of a network operator or handheld device.

What are the components of a wireless system?

- Handheld devices
- Connectivity, Coverage, and Gateways
- Middleware processing engine
- Transcoding
- API connection
- Data System Backend system



1- Handheld Devices

1. Thin Client devices, Palm, Workpad, Ipaq..
2. Two Way paging devices, like RIM
3. Smart-Phones, WAP phones
4. Others
5. Operating systems is a software program that manages the basic operations of a computer system.
 - a. Windows CE:
This is a light version of windows, developed by Microsoft. It is Installed on many of the PDA devices.
 - b. Palm OS:
It is developed by 3COM, proprietary platform. It is the most popular OS on the handheld due to the large market share that the Palm Pilot owns today. It supports some Java applications.
 - c. Linux: It is very promising for growth, open source base, Java friendly , very efficient, and it can be installed on many PDA devices and even on smart-phones
 - d. EPOC:
Symbian consortium drove the development of this operating system mostly for smart-phone devices used by Ericsson and Nokia. EPOC is one of the major operating systems in this market.

Each one of these handheld devices will require certain ways of communicating; they require their own Gateways to communicate to the application servers. Various sizes of screens create different data and screen layouts. Different keyboards generate different navigational options and different keys. The challenge is for the application server to sort out these devices, and send the data in the correct format to each handheld device.

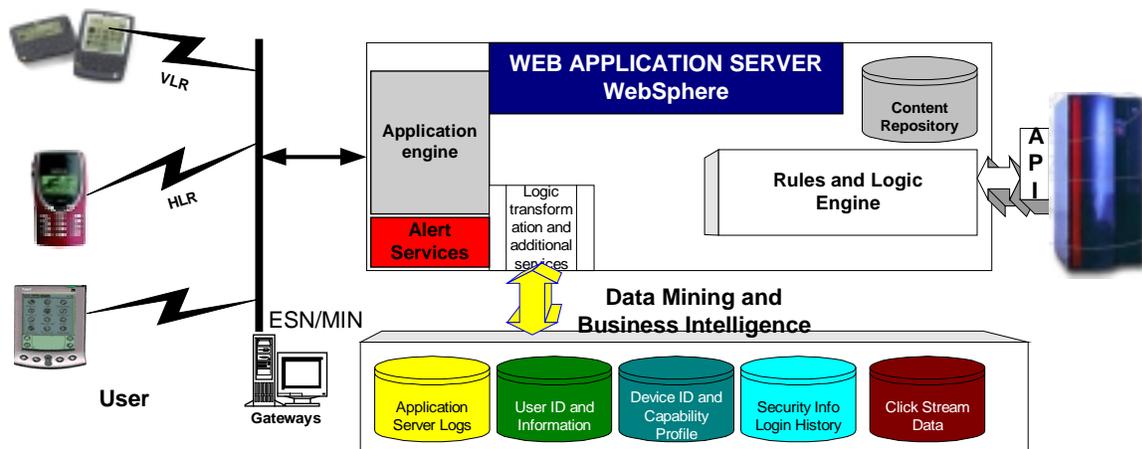
2- Connectivity, Coverage, and Gateways

In this section, we are going to explore the basic components of the wireless network architecture.

Starting from the end user, the handheld device can be any device that is used to access a local cell tower.

A cell tower is responsible for delivering local geographical coverage in a certain region. The coverage is divided into hexagonal boundaries.

The cell tower then sends the data to a Base Station. The data is then transferred to a switching center. The mobile switching center connects all Base Stations. The mobile network system will record, and identify all of the users information by Home Location Register (HLR), if the user is in the geographical network. If not, then the Visitor Location Register (VLR) will be tracking the call. This is when you pay



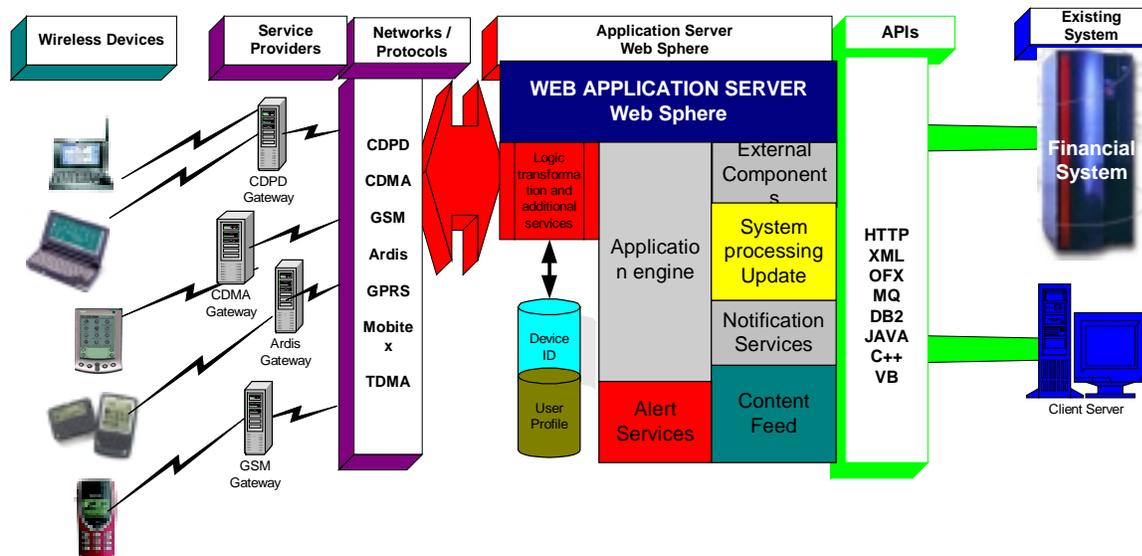
the big bucks for roaming. Once the call is initiated, the device will send its identity via its electronic Serial number (ESN) and Mobile Identity Number (MIN). This information is vital to have so the gateway can authenticate the user. This is where the application server can prepare the data to send back to the appropriate unit to be displayed.

A packet is a collection of data prepared in a specific way for transmission. There are two types of transmissions, circuit switched and packet switched. Circuit Switched is a dedicated circuit for communication between two dedicated devices. Its duration is for the entire call. Packet switching does not require a dedicated line between the sender and the recipient. This method enables the data to be divided into a number of packets and to be sent in different paths for its intended destination.

The connectivity will vary from one device to another, and from one service provider to another. The most challenging issue about the wireless systems is **coverage**.

As end users sign up with WSP (Wireless Service Providers), they quickly come to realize that the packages offered are not so perfect. Due to the limited coverage areas, it seems as if it's always the right plan at the wrong place.

Wireless service plans will vary in options as well as in cost. Some of the common protocols that the WSP support are GSM, (not so big in the US yet), CDPD, CDMA, Ardis...etc. All of which are trying to make it big. Wireless Service Providers are all jockeying for the position to be the global provider.



3- Wireless Middleware (Application server engine)

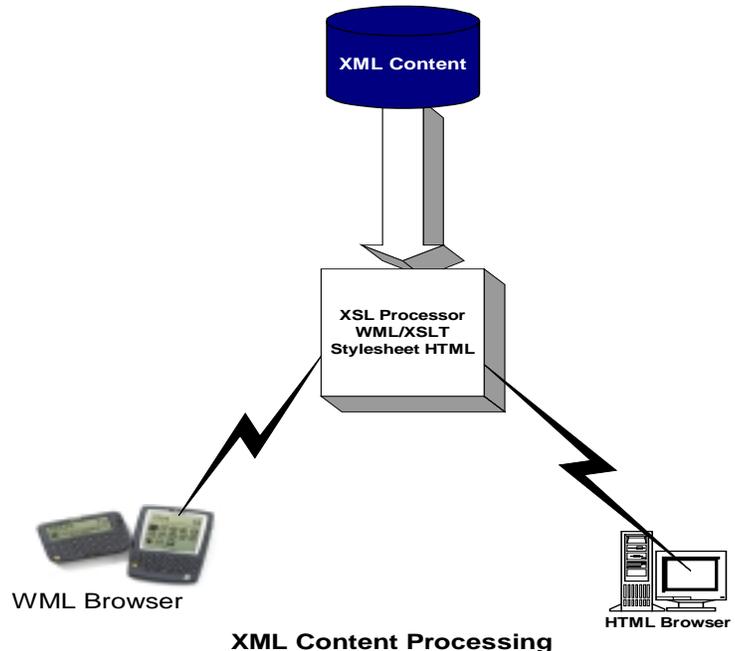
Wireless application is the focal point of the wireless system. This is where the flow of data is controlled, rules are set, and configuration files are executed. The application software should be an open system, easy to connect to and talk to other systems. One of the most common methods of communicating with backend systems is using XML API as the data delivery tool.

XML is used to extract and deliver data; XSL can perform the transformations, using the DTD files to execute the functions agreed on in the integration and design stage. Different handheld devices will have different screen templates. The Application server should be tracking the users sign-in by the device being used, in order for data to be presented correctly. The screen templates can be XML documents which conform to DTD files. The screen templates are used only to define the layouts of the screen. They are device specific.

4- Trans-coding, is it magic?

Transforming is the process of formatting the content (data) according to the handheld device request using XML, XSL style-sheets and DTD files. This method will enable the end-user to access data universally regardless of the device type.

Once a request from a handheld device is initiated, the application server will intercept the request to identify the device type and capture the content. Using several logical processes, the application server engine will process the data into an XML document, which can be communicated with the backend system via the API connection. The result of the requested data will be transformed (processed) using XSL style-sheets and then reformatted for the handheld device that made the request initially. This process can become complex very quickly, depending on the number of the handheld devices supported and the type of services offered by the financial institute. Therefore, products like IBM's WebSphere can be valuable tools to build a robust financial system in a short time. The WebSphere application server will handle the data dynamically and adapt it to the handheld device. Also it can run multiple applications and requests, and can be easily integrated to the backend system.



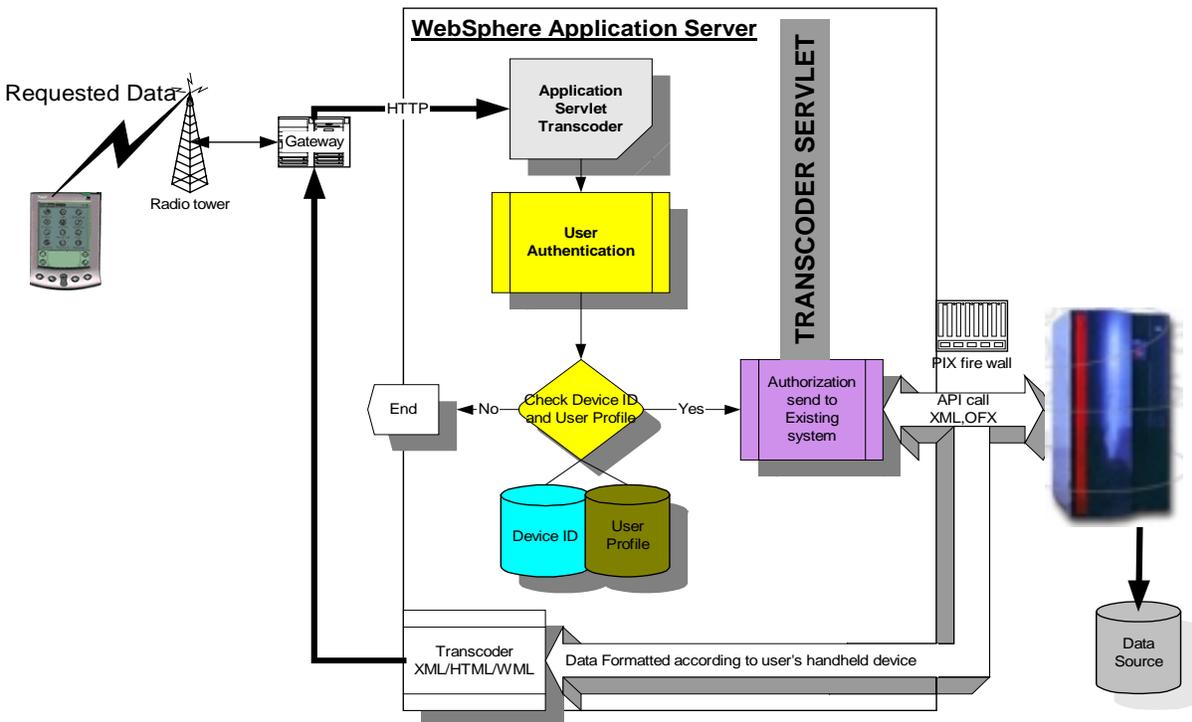
The WebSphere engine will select the correct screen template, format the data for the handheld device, and deliver the data requested. XSL is used for data transformation definitions, where the API will exchange the messages between the backend system and the application server. XSL and XSLT style sheets are mainly used to manage the presentation of the data, whereas the XML is handling the data.

Managing Data:

The application server can use common device characteristics to display the data. Using these standards can help in the development productivity.

User IDs and handheld device IDs are stored in the database at the application server level. The application server will access the database once a login request is received. The middleware database is used to prepare and format the data for the device requesting the login. The application server will also compare the registered device ID to the user ID for additional security verification. The application server communicates with the gateway server for the specific device that initiates the request. The gateway will push the information to the handheld device according to the connectivity platforms like CDPD, SMS, Mobitex, and CDMA.

The application server must accommodate for the different handheld platforms such as, thin client devices (IP based device), two-way paging, SMS messaging, and smart phones. It must then deliver the formatted data for that specific device data accordingly, end to end, in a reliable and secure manner.



Pushing or Pulling data?

Pull technology is when the handheld device initiates the communication using its gateway, requesting data. Then data is pulled from the application server down to the handheld device.

Push technology is when the application server is in more control over the handheld device. The application server will make decisions for the basic content and push data to the handheld device without waiting for the client's request.

In either, method authentication must take place first. The gateway transfers the handheld's request to the application server (middleware). The application server will then know the device type by its identifier. The information will be sent to the backend system of the financial institute, using the API between the application server and the backend system. The application server will receive the information from the backend system to report it to the handheld unit. At this time, the data will be formatted into appropriate screens for the device that requested the data. The data will be passed back to the wireless server provider gateway, and then back to the handheld device.

Wireless application Server must be device and network independent:

The wireless application server must be able to work with any of the networks offered by the Wireless Application Providers. The Application server should be:

- Easy to install, configure and add new services:
- The client application must be easy to install, customize, and add new handheld devices.
- Easy to Integrate with other servers and Back-End systems:
- Integration is one of the key steps for a successful implementation of the wireless project. The API of the existing financial institute's system must be reliable, and secure.

Open System:

The application server also must be an open system, using standard protocol to make it easier to add or change services, devices, and apply any customizations needed.

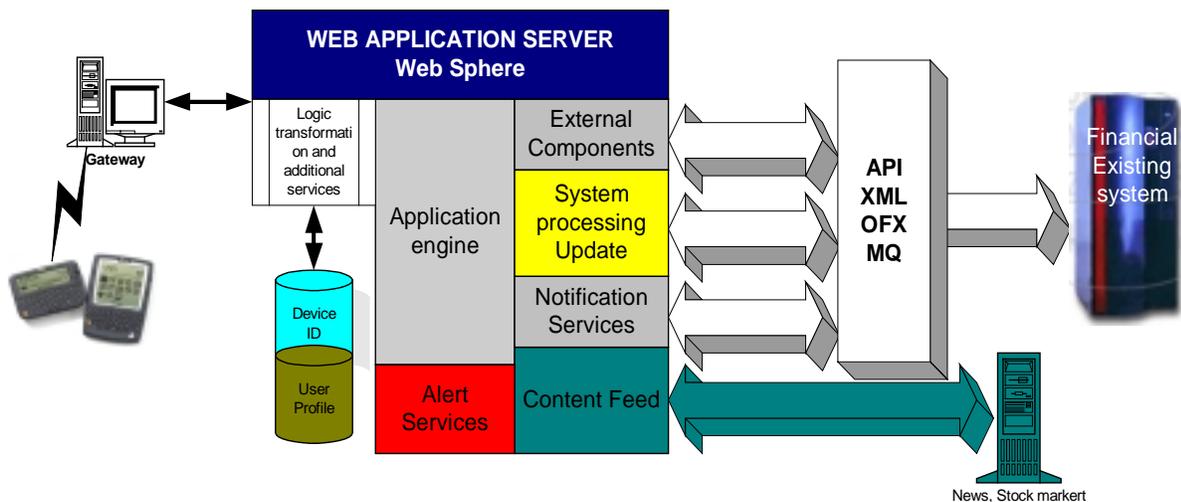
What about Screen Scrapping?

Screen scrapping is one method I would not recommend to use as a final solution. It's not a stable solution, due to maintenance required to keep updating the macro reader when fields are changed in the source document (Website). This method can leave more room for error. Screen scrapping is quick to implement, which can be a good tool for data presentation in the proof of concept stage.

The Wireless Application Server is not an Internet server nor an extension to the Internet:

The explosion of the wireless application industry in the last year or so has resulted in a common misconception. That is the wireless world is simply an extension to the Internet. While some wireless-enabling companies do use web-scraping (screen-scraping), a technique that captures screen content and transfers it to a wireless device. This technique tends to produce poor performance and unreliable wireless service. It's also more manual and maintenance intensive.

The most effective way to build a wireless application system is to connect into the back-end system, regardless of type. It could be a mainframe, client server, or a even Web-based system, using a direct connection via API.



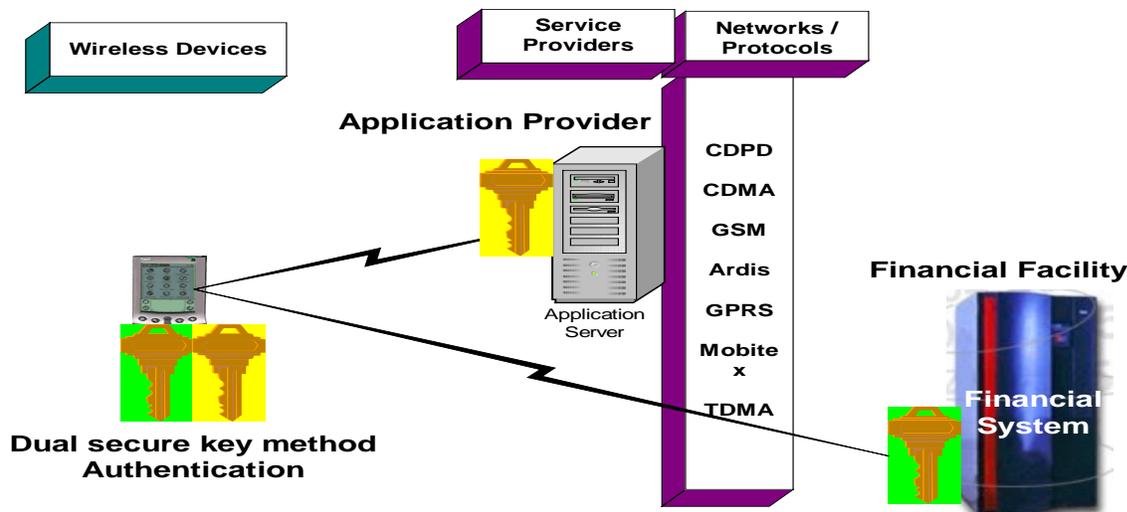
Security and Wireless Banking and Trading

Security is probably one of the most important issues in wireless banking, if not the most important.

A recent study on wireless banking security uncovered the main challenge facing both wireless banking innovators and online banking establishments; nearly 85 percent of respondents are worried about online security transactions, including credit card purchases. More than 90 percent expressed concern about revealing personal information online, such as social security numbers. Over 90 percent of proprietary cryptography has been broken. Cell phone systems have been hacked.

Wireless banking and trading is more vulnerable to attacks by hackers than many other wireless services. When data is flowing across a vulnerable environment, many of the available operating systems for phones and handheld devices offer little or no security. Most security violations occur within the institution or the service providers.

Customizing wireless security is extremely difficult, especially when computing power on the handheld devices is very limited.



Double key secure authentication is one of the protection methods used to verify access across different systems. Double key secure is where the user will authenticate two systems, the application server (at the Hosting service provider) and the financial institute. The transaction will be granted access, only when both locations agree.

Secure network architecture is achieved when all interaction points and data paths traveled, are implemented by using double secure keys.

It's proven this method of security can drastically reduce violations and system hacking internally and externally, because all three parties must agree. One of the more common securities used is PKI (Public Key Infrastructure), an encryption used for PDAs and Smart-phones security. PKI consists of two keys, a public key and a private key, used to authenticate the user and encrypt the data.

In addition, the financial institute should utilize the system to monitor access logs and flag questionable connections that can be done on the application server.

Encryption is a trade off between speed and security. A good rule of thumb is to encrypt on a 32-bit CPU at the rate of ten CPU clock cycles per byte. Look for the most compact software. It should run under 5,000 bytes of memory. Encryption can vary from one device to another, depending on the platform and the operating system. For additional protection, authentication can be implemented through user ID and password.

The Challenge

Wireless banking implementation is demanding. There are constantly changing standards for APIs, gateways, security methods, screens, operating systems, and browsers. There are also variable computing powers on the handheld devices and different bandwidth requirements.

Wireless banking can be risky, lengthy, and complicated to develop. APIs (interfaces) must be designed to connect to the existing backend system. The application server must be able to accommodate to all protocols and all devices. You never know which device the end user is going to use.

The application server must be able to communicate with all gateways, like WAP, GSM, two way paging, etc...

A product like Web Sphere can reduce development time drastically. Transcoding tested templates can make the developer's life much easier. The end result is a robust solution. Consulting companies promise a lot, but only few can deliver.

Since wireless banking is still at it's evolutionary stage, we must keep up with new technological advances, products, and development tools to help ease the transition.

The wireless network must be device and network independent. Most handheld devices have their own standards to deliver data across the data channels. The end user should be able to easily customize screens, alerts, notifications, and messaging request services. The system should be able to notify users regardless of the device type. Scalability is a major issue. Selecting the right platform to run the application server will dictate the available tools to work with. The wireless banking system must be an open system that can easily and reliably be integrated with new gateways to the backend system. This is a challenge not many banking institutions should undertake on their own.

The next best thing is out sourcing the development of the project, the implementation, and the hosting. Using a third party to administer and host the system is an option I would choose.

Selecting the right application vendor:

The vendor must have developed and installed a wireless financial system and must have a wide range of experience. Look for the following:

1. A trusted name and the longevity of the vendor is important
2. The vendor must have tested and used the product in a field specifically related to your field. For example, Wireless Trading is more demanding than Wireless banking. Wireless trading is time sensitive. Stocks, options, mutual funds, and bonds are all different services requiring different tools to process orders. The system must be able to deliver the data flawlessly and quickly to any handheld device. Wireless trading requires research capabilities. Wireless trading is much more active delivering user alerts, such as watch lists, quotes, charts, reports, notifications, summaries, and portfolio statuses. The wireless trading could be using external systems to gather data. The point is to be specific when dealing with application vendors; not all financial services are the same.
3. The testing and quality assurance stage must take place as early as possible to certify the systems. The application or applications must integrate fully to the backend system or systems, regardless of device type or platform. Management of all users definitions, events, requests, updates, changes, and requirements must be tested thoroughly.
4. Application servers must include monitoring tools and protocol management of all requests.
5. A turn key solution is an end-to-end solution. It goes from the backend system, where the data source resides, to the API connection, to the application server, to the WSP gateways, and then to the handheld units.

6. The vendor must have widely available resources and experienced programmers, systems architects and project managers. Additional manpower must be available immediately if needed.
7. References and physical site visits are key to comprehend the consulting, development, and hosting environment. The consulting company will be an extension of your business. This is the life link between you (your system) and your customers using the services.
8. Backup and catastrophe planning must be in place.
9. The wireless application system must be network and device independent. The application should be fully configurable with customizable screens, using standard API's. The wireless application server must be an open, modular architecture, to provide the user with the maximum flexibility and extensibility to make the development and deployment easier.
10. Development tools to enable you to make changes, add services, or deploy applications are crucial.
11. Products like IBM Web Sphere are End-to-End Solution for the wireless banking and trading enterprise. The IBM Web Sphere solution and Web Sphere Everyplace Suite are highly scalable server software, and have development tools for connecting millions of wireless devices to the Web. Java is capable to transcode, encapsulate the application logic, access XML documents, XSLT style sheets, and define the presentation. The Web Sphere architecture will help the programmer to focus on providing high quality. Web Sphere can handle the presentation and data management without getting involved in dynamic content generation. Views and screens can be developed for different devices easily and quickly using the same application logic.

The road to a successful implementation:

Remember, wireless users will not be able to multitask using the handheld devices; therefore, easier navigation will play a major role in the success of the project. It's crucial to test all users' functionality thoroughly, no matter how tight the schedule is for implementation. Depending on the type of network to be implemented, number of markup languages, and handheld devices to be supported. Testing can be cumbersome and complex. It is always a good idea to use multiple software development tools to test for the real world users. The financial institute should make use of the following steps for implementation and testing:

1. Documentation, Documentation, Documentation!! (in this order). Document all rules, procedures, and specifications.
2. Setup the application network environment as early as possible. Start with high-level conceptual and visual design.
3. Run traffic studies on bandwidth required to communicate between the backend system and the middleware system (application server), the gateways.
4. List all users functions and requirements.
5. Perform user analysis.
6. Perform technical assessment.
7. Hold users group meetings.
8. List business requirements.
9. Define functional requirements.
10. Definition of performance requirements hardware and software.
11. Use a standard API like MQ, or OFX (common in the banks industry), or develop XML API, which is becoming more popular.
12. Design business performance and process requirements.
13. Develop delivery plan.
14. Build a proof of concept to test all systems functions and requirements. Test APIs and architectural designs of the applications. Integrate with the data source (existing system) directly.
15. Start with a pilot (limited users).
16. Fix bugs, and fine tune systems performance.
17. Implement the full-scale rollout.

Conclusion

We must react to the new world economy quickly and offer what the clients are looking for!! The future of wireless banking is massive and aggressive in terms of requirements, demands, and support. The good news is, it's great for financial business, but we must be cautious in implementation and execution to deliver a reliable service.

Wireless media is challenging. Many variables are not under control yet. Coverage is a big hindrance. Legacy systems with different topologies and different platforms make things even tougher. There will be more streamline markets demanding new ways of conducting transactions.

The future of wireless banking and trading has promising magnitudes of growth. Jupiter Research expects 18 million more people in the United States will become wireless subscribers in 2001, increasing the total number to 128 million. Moreover, the percentage of subscribers with Internet-ready wireless handsets will quadruple during this year.

Despite millions of new users, the wireless market can expect some real challenges in the near future. "While penetration of wireless data services will gain momentum in 2001, a lack of substantial new technology deployments in the United States will stifle true innovation. Location-based services, high-speed networks, and highly sophisticated handsets will remain elusive in 2001."

Wireless banking is sensitive to security, and is essential to finding the right balance between speed and encryption. Accuracy, consistent availability, and reliability of the services are key to a successful implementation and survivability of the financial institute.

Geographical coverage is imperative to successful implementation. It must be clearly defined and understood. The confirmation of transactions is key to show the level of commitment and accuracy to your customers.

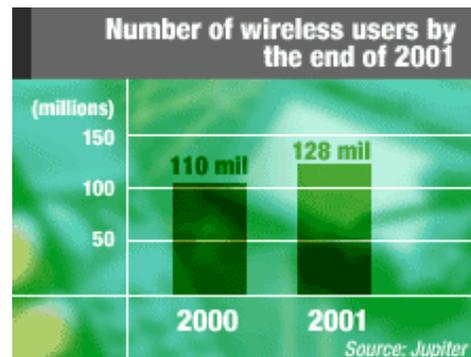
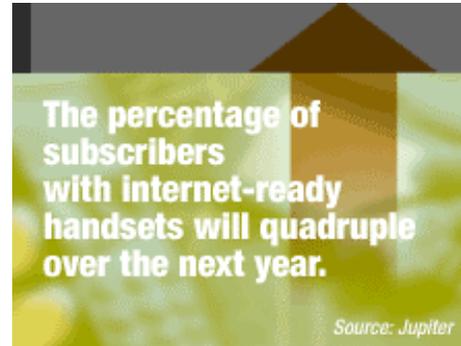
Wireless banking is greatly dependant on the efficiency of the bandwidth. The more efficient the bandwidth, the faster the content is downloaded. End-users requirements are driving a demand for faster transmission and higher bandwidth capacity.

In order to offer an enterprise wireless solution, major consortiums of the industry must break all political barriers and agree to a global format of communication. The consortiums must arrive at solution that can access all platforms across all networks regardless of device type, much like the Internet.

The financial institutions are between a rock and a hard place. They would like to extend their services to the wireless world, but they lack the resources and the expertise to implement and deliver to their customers in a timely manner.

Therefore, out-sourcing can be a vital option for the following reasons:

1. The financial institute can focus on their core business.
2. Extend the product offering in a timely manner, and get to the wireless market place sooner.
3. Outsourcing will help predict cost better, and forecast more accurate budgeting.
4. Use of the latest in technology.



Benefits of WebSphere middleware application server:

- The financial institute can extend the reach of its product to new markets in a much shorter time.
- Communicate with handheld devices seamlessly to access data and applications.
- Enhance data transfer using the load balancing function, which can detect bandwidth capability and optimized data streams.
- Reliable systems processing, and commanding encryption.
- Sophisticated monitoring tools.
- Reduces development time greatly.
- Scalable open architecture using XML and XSL standards.
- Integrates easily to backend systems, such as Mainframes and Client servers.
- Unmatched product support.
- End to end solution.

Wireless banking and trading must be a virtual and global solution. Competitive forces will shape the wireless banking industry and help deliver the offerings desired to the end users.

Wireless banking must reach a global standard before it can be unleashed to it's greatest potential.

API	Application Programming Interface
CC/PP	Composite Capability/ Preferences Profiles
CDMA	Code Division Multiple Access
CGI	Common Gateway Interface
CPI	Capability and Preference Information
DCS	Digital Communications System
DTMF	Dual Tone Multi-Frequency
FDD	Frequency Division Duplex
GPRS	Global System for Mobile Communications
GSM	Global System for Mobile Communication
HTML	Hyper- Text Mark-up Language
HTTP	Hyper-Text Transport Protocol
JDBC	Java Database Connectivity
JSP	Java Server Pages
PCS	Personal Communications System
PDA	Personal Digital Assistant
PDC	Personal Digital Cellular
PeMS	Personalized e-Messaging Server
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
RDF	Resource Description Framework
SMS	Short Message Service
SSL	Secure Sockets Layer
TDD	Time Division Duplex
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
WCMP	Wireless Control Message Protocol Wireless
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformation
WTA	Wireless Telephony Application
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security