

Mobile Computing Strategy for State Government

Wireless mobile devices, such as smartphones, and the technologies that they bring along with them are relatively new to this area. They are quickly gaining momentum as a viable business solution for mobile employees who want to stay “connected” to their office while they are away. Now that cellular phones are no longer just voice devices, they offer a potential for mobilizing workers in ways not available in the past.

However, to truly unleash the full potential of these devices, you need more than just the device. There is some basic functionality that is available via desktop versions of their software, but the features that are added by implementing a backend server infrastructure really make them useful. Therefore, in order to do a fair comparison between the devices and their capabilities, this study was performed with all three units having that backend server infrastructure in place. For the BlackBerry devices, BlackBerry Enterprise Server was used and for the PocketPC, Palm devices, two server products were evaluated; GoodLink by Good Technology and Mobile Suite by Intellisync (See Appendix A for the test configuration).

The study team came up with 22 business requirements that were determined to be good testing criteria for the devices. These requirements were then prioritized based on how vital they were to the solution. Hardware specific requirements were automatically prioritized as “Desired”, but not required, as it was felt that those types of things would be changing with each new release of the device and therefore had no bearing on how the unit provided the required functionality. (These business requirements, including their priority and the results of our testing can be found on Appendix B).

BlackBerry

The BlackBerry handheld devices are extremely capable when it comes to wireless email. Their interface is simple to navigate and can be customized somewhat in order to meet the user’s needs. The telephone allows for using your synchronized address book (Outlook contacts) as your phone book and the internet browser is “no frills” but adequate in most scenarios.

They offer encryption of the data while in transit between the handheld and the server (or desktop in the case of redirector installs) and can be password protected in order to protect against unauthorized use. While “locked” the device cannot be accessed via the screen or the cradle without entering the password and data on it will be erased if 10 unsuccessful passwords are attempted. There is also an option to encrypt the data on the device, when the screen is locked.

When used in conjunction with the BlackBerry Enterprise Server (BES), these devices offer a lot of additional functionality. Again, their strong points still center on wireless email, however, when accessing a server on the backend, Personal Information Manager (PIM) synchronization and email reconciliation (processing of email deletions) can also be done wirelessly. The attachment service allows for the reading of several popular attachment types (ie. word, excel, .pdf, etc.) and the ability to accept and decline meeting invitations also becomes available via the server. Administrative policies can be used to force such things as password protection, on-device encryption, and limit what additional software can be installed on the device. It also allows for disabling the email redirection and remotely erasing a device if it is lost or worse yet stolen.

Some custom applications can be written that take advantage of the Mobile Data Service portion of the server and allow for accessing corporate data via the devices. The data does not have to be exposed to the public internet. The device is configured to use the BES as a proxy or Virtual Private Network (VPN) gateway in order to access data that remains securely behind the firewall.

Although the BlackBerry and BES combination offers a lot of functionality when it comes to email and PIM synchronization, they aren’t quite as full featured with their other options. As

stated above, they have a “no frills” browser that is adequate in most scenarios, for most people. However, a power user would want a more capable browser. They also lack the ability to save attachments off of email onto a local store on the device and as of right now none of their devices available in this area offer external storage options (ie. secure digital media, etc.). Probably the largest drawback for the BlackBerry platform is that it is so proprietary. The BES can only service BlackBerry handhelds and BlackBerry handhelds can only be serviced by the BES. Therefore, if BlackBerry handhelds are going to be supported, you must use a BES in order to provide the server infrastructure.

Palm and PocketPC

Palm and PocketPC devices are also extremely capable devices and offer some things that the BlackBerry is lacking. The Palm has a more functional browser and has the ability to save attachments to the local store of the device. Additional software is available that will also allow word processing and spreadsheet capabilities on it. This allows for the creating and editing of documents on the device.

The PocketPC has the most robust web browser of the three and it also has the ability to save attachments to the local store of the device. PocketWord and PocketExcel are installed by default, which offer compatibility with the desktop versions of Word and Excel. And a native Terminal Services client is appealing to Information Technology personnel who may need to use the device to remotely administer servers, etc.

Server infrastructures can also be utilized with these in order to provide the same additional functionality as the BES offers to BlackBerry users. Due to the extra capabilities of the handhelds, most of the drawbacks to the BlackBerry (+BES) solution are not issues with these solutions. Two such servers are; GoodLink by Good Technology and Mobile Suite by Intellisync.

GoodLink

GoodLink can provide the “BlackBerry experience” to PocketPC and Palm devices. It installs a GoodLink client, which is used as the default mail program rather than the one that ships on the device. This client offers full wireless email and PIM synchronization, the ability to read attachments, and the ability to accept or decline meeting invitations. It also offers additional features such as flagging messages for follow up, a preview pane for reading email, and lookups against the Exchange Global Address List.

GoodLink also provides data encryption during transmission as well as the use of administrative policies to force password protection and wirelessly update encryption keys to increase security. If a device is lost or stolen, its data can be remotely erased in order to ensure it is safe from unauthorized access. Additional administrative control is also available via wireless provisioning of devices, custom application deployment, and role based administration.

Good Technology also offers the ability to write custom applications that take advantage of their data service piece, known as GoodAccess. GoodAccess allows for the writing of applications that can access corporate data via the devices. This data is not exposed to the public internet; instead the device is configured to use the GoodAccess portion of the GoodLink server as a proxy or VPN gateway in order to access the data.

A development tool is provided which allows a developer to rearrange a web application's pages to a size and layout that is more suitable for the window size of a mobile device. The mobile device will execute this application via the device's Good Browser which connects to the GoodAccess server. The GoodAccess server acts as a proxy between the client on the end user's device and your enterprise application server. This allows the GoodAccess server to maintain the validity of information being passed between the client and application server. Thereby, if the mobile device goes in and out of service as you travel from location to location, your server session is persisted by the GoodAccess server. Good Technology's management tool allows third-party or custom applications to be deployed to a device based on managed security groups

Mobile Suite

The Mobile Suite consists of four modules that can be used separately or in any combination. These four modules; Wireless Email, Mobile Systems Management, File Sync, and Data Sync combine to provide the service to handheld devices based on what the needs are.

The Wireless Email module provides the “push email” or “BlackBerry experience” to PocketPC and Palm devices. The wireless synchronization of email and PIM information is all handled by a client that is installed on each device. This client runs in the background, and the user continues to use the mail and calendaring clients that are native to their device's OS, which provide the ability to read attachments and accept or decline meeting invitations. This module also offers for the encryption of the email messages while in transit between the device and the Mobile Suite server.

The Mobile Systems Management module provides the device security and control features. It allows for administrative policies to be set to force password protection and “on device” encryption to ensure that the data is encrypted as long as the device is locked. If a device is lost or stolen, data can also be wiped remotely to ensure that it is safe. Additional administrative features available include wireless provisioning of devices, role based administration, and user groups.

The File Sync and Data Sync modules can be used in order to provide access to corporate data via the devices. This data is replicated to the device, where it is used by applications, etc. Changes are then synchronized back to the servers that reside behind the firewall, by using the Mobile Suite server as a proxy or VPN gateway. The File Sync module is used to publish and synchronize office documents and web content. The Data Sync module is used for synchronization of databases, etc.

Support

As with any technology being introduced into State Government, support is a major concern and one that should play a large factor in deciding what types of devices should be used and more importantly, how they should be used. Gartner suggests a “three level support model” for mobile devices (1):

- Level 1 – PC-equivalent support (Trusted).
- Level 2 – PIM/e-mail-only support (Tolerated).
- Level 3 – No support (Despised).

Devices that fall into the Level 1 category would be fully supported similar to the way that PCs and notebooks are today. Custom written applications would be written for devices at this level, and support for the applications would only be available for these devices. In order to provide this level of support, a platform and a device must be selected as the business standard. Deviations from that standard platform/device would automatically fall into one of the other two levels.

Level 2 provides for supporting the applications that run on the devices, rather than the device itself. For devices that are not part of the Level 1 tier, a support strategy would be set to allow for their use, as long as they run the software that was selected by the business. So, if people wanted to use their own personal devices, or any device that does not fit into the Level 1 tier, they could as long as they ran the supported application for the functionality they required (such as PIM/email). By forcing the use of the business standard software, rather than the software that shipped with the device, policies could be enforced which would allow some control over the data that is being transferred to these devices. This level is greatly dependent on business standard software being selected that supports a wide range of devices.

Devices that do not meet pre-determined Level 2 minimum criteria automatically fall to the Level 3 category. These devices would not be supported by the business and therefore would not be able to take advantage of the server infrastructure that is in place. It is crucial that user expectation for these devices be set up front so that they are aware that if they choose to

purchase this type of device, their options for using the device for business purposes will be extremely limited.

Application Development

Wireless mobile devices provide access to two types of applications: rich client and browser based web applications. Rich client applications are installed on the device and web applications which run through a browser application preinstalled on the device.

Rich client applications are developed using either Java 2 Micro Edition (J2ME <http://java.sun.com/j2me/index.jsp>) or the Microsoft .Net Compact Framework (<http://msdn.microsoft.com/smartclient/understanding/netcf/>). J2ME applications are supported on many more mobile devices than the Microsoft .Net Compact Framework applications. J2ME is supported on all three of the evaluated devices (Blackberry, PocketPC, and Palm). The Microsoft .Net Compact Framework is currently only supported on the PocketPC. However, Palm will support the Microsoft .Net Compact Framework in the future as Palm switches from its own operating system to the Windows Mobile platform.

Selecting a development platform will need to be determined on an application by application basis. J2ME is available on more devices. However, neither J2ME nor .Net Compact Framework is a more superior platform for all business application types. The target device type will most likely determine the platform along with your developer's skill sets. The enterprise will most likely support both platforms.

Security

Mobile devices of any kind, bring with them some inherent risk that must be considered when deciding how they should be used. Points of concern are the security of the data during transmission, security of the data while it is on the device, and security of the device in the case of loss or theft. All of these concerns can be addressed if the server infrastructure is utilized and configured properly. If desktop versions of the software are used in place of the server infrastructure, not all of these concerns can be addressed.

Security of the data during transmission is accomplished through encryption. All data intended for the handheld is encrypted by the server, using the device's encryption key. That way, the only device that can decrypt the data is the device that it was destined for. If for any reason the data is intercepted in transmission, it is unreadable due to the lack of the decryption key. Likewise, all data intended for the server is encrypted using the server's encryption key and therefore only the server can decrypt it.

Security of the data while it is on the device can be tricky. We have to assume that at least some of the data that is stored on the device is of a confidential or business critical nature. Therefore, protecting it once it is on the device is crucial in order to protect against unauthorized reading, forwarding, replying, etc. All three server products allow administrators to force a password policy for the device. Once locked, a user would need to type in a password in order to access any of the data that is on the device. While the device is locked, USB or Serial Port access to the device is also disabled, so someone could not plug the device into a computer in order to access the data. Two of the three products (BlackBerry Enterprise Server and Intellisync Mobile Suite) also offer encryption of the data on the device while the password is locked.

Security of the device in case of loss or theft can be addressed in a couple of different ways. When password protected, devices can be configured to delete their data after a specified number of unsuccessful logon attempts. This feature provides some level of security, but an even more effective way to deal with this situation is the ability to remotely erase data or even perform a hard reset (delete all applications, data, etc. and return the device to the factory defaults) of the device.

Financial Requirements

Regardless of which device or server infrastructure chosen, a substantial financial investment will need to be made in order to utilize these types of devices and provide proper support for them. Desktop versions of the software would bring down the cost, but also limit their use substantially and provide much less security control over the devices. These required investments are outlined, in detail, for each product in Appendices C-E and include:

1. Handheld hardware
2. Cellular carrier fees
3. Server hardware and hosting fees
4. Software licensing fees
5. Software maintenance and support

Recommendation

Mobile workers are always looking for ways to stay connected to their business while they're away. Wireless mobile devices are emerging as a tool that can supply that connectivity, allowing workers to always know what's going on back at the office. As the use of these devices increases, that remote connectivity is becoming required rather than optional. Along with that, the desire for increased functionality is also growing rapidly. State Government's mobile workforce is currently most concerned with wireless email functionality. The ability to always have a current inbox and calendar at their fingertips is driving the need for an enterprise wireless email solution.

That wireless email functionality is easily achievable with any of the solutions that were evaluated, using any of the three devices. However, it is crucial that this functionality is rolled out in a manner that will not threaten the security of corporate data and will not be prohibitive to the future use of these devices for expanded functionality (ie. custom applications). Therefore, it is the opinion of the study group that limiting the enterprise supported use of these devices would be a mistake at this time.

These devices are changing at an extremely fast pace right now and are constantly adding features in order to make them more appealing to consumers. As this happens, the "latest and greatest" device is always changing. In most cases, these devices are not only used for business related functions, but for personal as well. Therefore, enterprise support (or the lack there of) is not enough of a deterrent to stop someone from buying that "cool" device that has everything they want. Instead, they're more likely to purchase the device and use it via desktop software, which carries with it inherent security risks.

Level 2 of the Gartner recommended three level support model provides for supporting the applications that run on the devices, rather than the devices themselves. This allows for the broadest range of devices. The study group feels that this would be the best strategy for State Government right now. The configuration would allow the State to define any device that can run the required software as a Level 2 device, and therefore supported by the enterprise. If a device cannot run the software, then it cannot be added to the server infrastructure and therefore will not be supported (a Level 3 device as defined by Gartner). This configuration would also allow for a future Level 1 type of device, if it becomes necessary.

Gartner's Level 2 support also provides for the use of personal devices, as long as they can run the enterprise software. The study team agrees with this and recommends that personal devices be allowed onto the enterprise server infrastructure; as long as the user understands that all devices must comply with the administrative policies that are being applied by that system. By allowing the use of these personal devices, the State can ensure that the corporate data that resides on them is protected against unauthorized access both while in the employee's possession or in the case of loss or theft

This approach does require server infrastructures that can support a variety of devices. Both GoodLink and Mobile Suite can support several devices, including the PocketPC and Palm devices currently being offered by the local cellular provider. As the testing results illustrate (Appendix B), the functionality between the two server products, for the most part, is

equal. They both meet all of the business requirements that were defined as “Core” or “Essential” and also offer most of the additional functionality that was defined as “Desired”. Although they do approach application development differently, neither of the approaches would be prohibitive to development of mobile applications in our environment.

The study group believes that both of these two server offerings will meet our current business needs. However, the financial requirements for the two products are quite different (Appendices D-E). GoodLink offers a lower upfront cost, but the monthly charges associated with it are higher than that of the Mobile Suite offering. Therefore, it is the recommendation of the study group that Mobile Suite be selected as the server infrastructure for devices that use the PocketPC or Palm operating systems, as over time the lower monthly charges will make up for the higher upfront cost.

BlackBerry devices are not supported by either GoodLink or Mobile Suite. However, they offer the functionality desired by most (wireless email/PIM synchronization) at a lower price than the other two platforms. Even though they run on a proprietary platform, they offer too much business value to be considered a Level 3 device. Therefore the study team believes that these devices should also be included as Level 2 devices and the required infrastructure (BlackBerry Enterprise Server) should be built to support them.

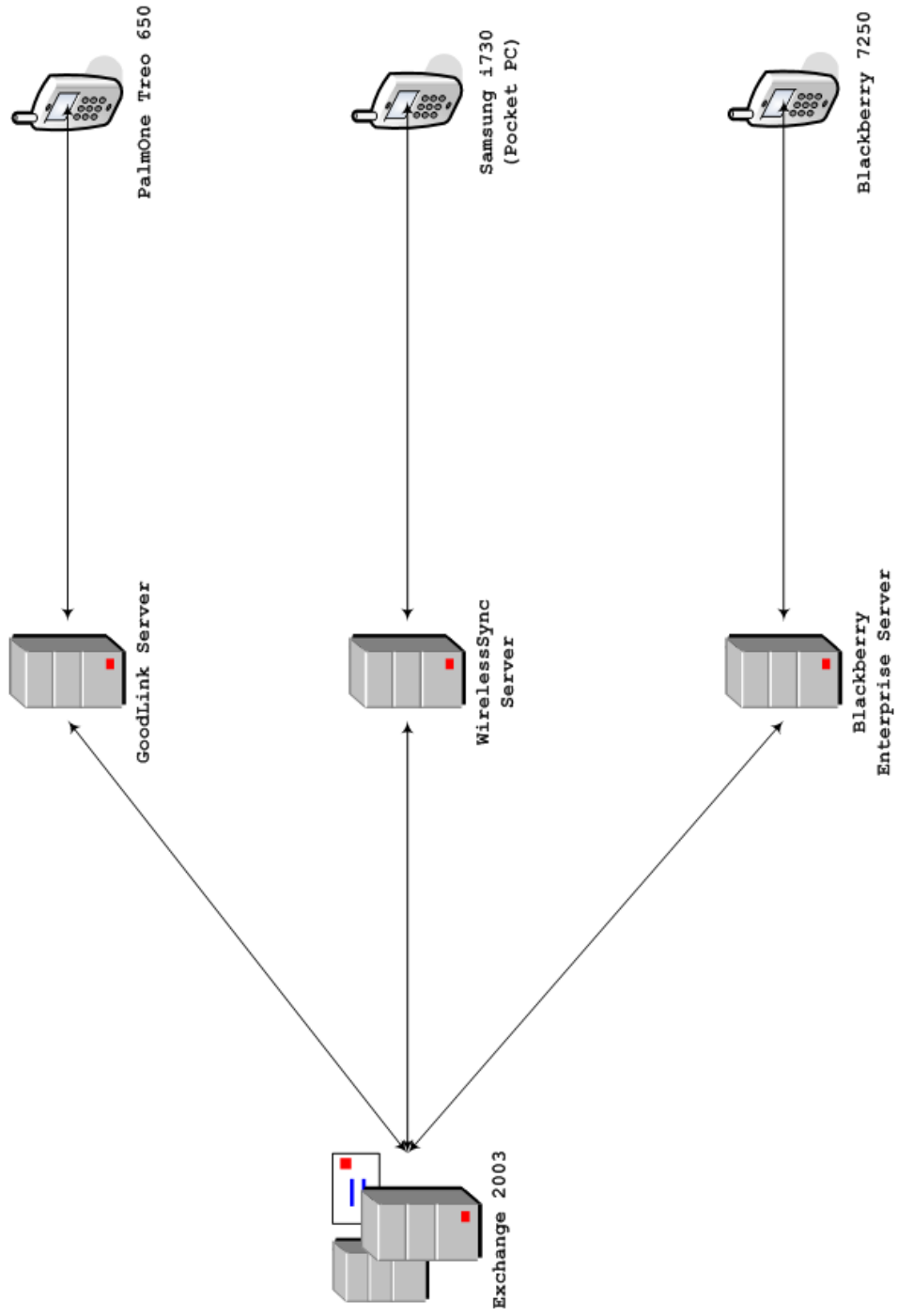
By offering multiple platform choices for mobile workers, the State would offer the device flexibility necessary to mandate server usage, which is vital for the security of corporate data. It also would position itself well for potential use of mobile devices in the future.

References

(1) Gartner: “Key Advice on How to Support PDAs and Smartphones in Business”. April 20, 2005

Handheld Device Test Configuration

Appendix A



Appendix B

TESTING RESULTS OF THE IN SCOPE REQUIREMENTS

Type	Business Function / Category	Requirement	Priority	Blackberry (w/BES Server)	Palm (w/GoodLink Server)	PocketPC (w/Wireless Sync Server)
Functional	Office Automation	Wireless Email (send & receive)	Core	Yes	Yes	Yes
Functional	Office Automation	Wireless Calendar Syncing	Core	Yes	Yes	Yes
Functional	Office Automation	Wireless Contact Syncing	Core	Yes	Yes	Yes
Functional	Office Automation	Ability to accept or decline meeting invitations from device	Core	Yes	Yes	Yes
Functional	Office Automation	Ability to read attachments on the device	Core	Yes	Yes	Yes
Functional	Office Automation	Web Browsing	Core	Yes	Yes	Yes
Functional	Office Automation	An "All in One" device	Core	Yes	Yes	Yes
Operational		Ability to control the distribution of apps to devices	Essential	Yes	Yes	Yes
Operational		Ability to configure device policies	Essential	Yes	Yes	Yes
Operational		Ability to remotely erase device	Essential	Yes	Yes	Yes
Technical		Ability to support devices on multiple cellular carriers	Essential	Yes	Yes	Yes
Functional	Office Automation	Wireless Task Syncing	Desired	Yes	Yes	Yes
Functional	Office Automation	Wireless Notes Syncing	Desired	Yes	Yes	Yes
Functional	Office Automation	Ability to save attachments to the device	Desired	No	Yes	Yes
Functional	Office Automation	Ability to create and edit documents on the device	Desired	No	Yes	Yes
Functional	Office Automation	Ability to send an attachment from the device, through the server	Desired	No	No	Yes
Functional	Office Automation	Additional Memory Slots	Desired	No	Yes	Yes
Functional	Office Automation	Ability to run other custom apps	Desired	Yes	Yes	Yes
Functional	Office Automation	Camera in device (both video and still shot)	Desired	No	Yes	No
Functional	Office Automation	GPS	Desired	No	No	No
Operational		Ability to provision a device wirelessly	Desired	Yes	Yes	Yes
Technical		Ability to access internal data from the device without making it externally available	Desired	Yes	Yes	Yes

Appendix C

BlackBerry Pricing

25 Users			
<u>One Time Costs Per User</u>		<u>Ongoing Monthly Costs Per User</u>	
RIM 7250 Device	129.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
BES Software + CAL	150.00	450 anytime minutes	
Total	279.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 25 Users)	\$12.00
		Blackberry Software Maintenance & 24x7 Support	\$5.00
		Total	\$82.00
50 Users			
<u>One Time Costs Per User</u>		<u>Ongoing Monthly Costs Per User</u>	
RIM 7250 Device	129.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
BES Software + CAL	105.00	450 anytime minutes	
Total	234.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 50 Users)	\$6.00
		Blackberry Software Maintenance & 24x7 Support	\$4.00
		Total	\$75.00
100 Users			
<u>One Time Costs Per User</u>		<u>Ongoing Monthly Costs Per User</u>	
RIM 7250 Device	129.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
BES Software + CAL	80.00	450 anytime minutes	
Total	209.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 100 Users)	\$3.00
		Blackberry Software Maintenance & 24x7 Support	\$3.00
		Total	\$71.00
120 Users			
<u>One Time Costs Per User</u>		<u>Ongoing Monthly Costs Per User</u>	
RIM 7250 Device	129.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
BES Software + CAL	75.00	450 anytime minutes	
Total	204.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 120 Users)	\$2.50
		Blackberry Software Maintenance & 24x7 Support	\$2.50
		Total	\$70.00

***This pricing includes Wireless Email / PIM synchronization as well as the Mobile Data Access component of the BlackBerry Enterprise Server.

Appendix D

GoodLink Pricing

25 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
GoodLink Software + CAL	\$160.00	450 anytime minutes	
Total	\$509.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 25 Users)	\$12.00
		Software Maintenance & 12x5 Support	\$3.00
		GoodLink Subscription Fee (\$240.00 / 12)	\$20.00
		Total	\$100.00
50 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
GoodLink Software + CAL	\$130.00	450 anytime minutes	
Total	\$479.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 50 Users)	\$6.00
		Software Maintenance & 12x5 Support	\$2.50
		GoodLink Subscription Fee (\$240.00 / 12)	\$20.00
		Total	\$93.50
100 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
GoodLink Software + CAL	\$115.00	450 anytime minutes	
Total	\$464.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 100 Users)	\$3.00
		Software Maintenance & 12x5 Support	\$2.00
		GoodLink Subscription Fee (\$240.00 / 12)	\$20.00
		Total	\$90.00
120 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
GoodLink Software + CAL	\$112.00	450 anytime minutes	
Total	\$461.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 120 Users)	\$2.50
		Software Maintenance & 12x5 Support	\$1.75
		GoodLink Subscription Fee (\$240.00 / 12)	\$20.00
		Total	\$89.25

**One Time Costs would go up by \$90 if the device would be the Samsung i730 (PocketPC Device) because its cost is \$439.99

***This pricing includes Wireless Email / PIM synchronization. Mobile Data Access functionality can be achieved through an additional server component (GoodAccess) which would incur additional licensing and maintenance charges.

Appendix E

Mobile Suite Pricing

25 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
Mobile Suite Software + CAL	\$250.00	450 anytime minutes	
Total	\$599.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 25 Users)	\$12.00
		Software Maintenance & 12x5 Support	\$7.00
		Total	\$84.00
50 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
Mobile Suite Software + CAL	\$250.00	450 anytime minutes	
Total	\$599.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 50 Users)	\$6.00
		Software Maintenance & 12x5 Support	\$4.00
		Total	\$75.00
100 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
Mobile Suite Software + CAL	\$250.00	450 anytime minutes	
Total	\$599.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 100 Users)	\$3.00
		Software Maintenance & 12x5 Support	\$4.00
		Total	\$72.00
120 Users			
One Time Costs Per User		Ongoing Monthly Costs Per User	
PalmOne Treo 650 (Palm OS Device)	\$349.99	Verizon Voice & Data Bundle - "Core Choice for Business"	\$65.00
Mobile Suite Software + CAL	\$250.00	450 anytime minutes	
Total	\$599.99	Unlimited IN Calling minutes	
		Unlimited Night & Weekend minutes	
		ITD Hosting Fee (\$300 / 120 Users)	\$2.50
		Software Maintenance & 12x5 Support	\$4.00
		Total	\$71.50

**One Time Costs would go up by \$90 if the device would be the Samsung i730 (PocketPC Device) because its cost is \$439.99

***This pricing includes Wireless Email / PIM synchronization. Mobile Data Access functionality can be achieved through additional server modules (DataSync and FileSync) which would incur additional licensing and maintenance charges.