Business Summary

Rosetta-Wireless Corporation
1 TransAm Plaza Drive – Suite 420
Oakbrook Terrace, IL 60181

August 16, 2004

Introduction

This is the information age, with corporate global performance dependent on leveraging huge databases of enterprise information. The advantage goes to those companies that enable their diverse, distributed workforces to have all current information that they need, exactly when and where needed, securely and economically.

But only personnel on enterprise campuses enjoy the rich environment of *immediate, secure and economical access to complete, up-to-date enterprise information.* Off-campus, mobile workers are limited to receiving minimal text-based information or suffering slow downloads via multiple, fragmented access technologies.

Moreover, mobile workers have no prospect of ever participating in the rich enterprise information environment because all current and future (e.g., 2.5-4G, WiFi, WiMax, EV-DO) wireless networks have systemic limitations that preclude ubiquitous sharing of enterprise information.

But now, WIPS™, the Secure Mobile Enterprise™ system developed by Rosetta-Wireless Corporation, permanently extends the enterprise information environment to all mobile workers. Unlike piecemeal wireless data solutions (e.g., Blackberry, GoodLink, AT&T M-Life), WIPS is the *complete, enterprise-grade* solution, working over multiple wireless networks and with all wireless access technologies to deliver all critical enterprise information instantly, securely, and affordably, whenever and wherever needed.

Because of its easy scalability, initial WIPS deployment will be as a wireless carrier data service operating over existing equipment and networks, with a target launch in 2005. Later, the Secure Mobile Enterprise platform also will enable "must-have" solutions for a broad range of wireless data requirements, such as large enterprises, homeland security, healthcare, and vehicle telematics markets.

Unfulfilled Demands of Enterprise Mobile Data Market

Demand for enterprise mobile data technology is driven by the information needs of mobile workers and by wireless carriers' need for new revenue sources.

Mobile workers[1] are defined as those who spend more than 20% of their time off enterprise campuses. In the U.S., there are about 55 million mobile workers, representing about 25% of worldwide mobile workers. Worldwide, the number of mobile workers is expected to roughly double over a five-year period to over 400 million by 2008.

There is a wide variety of mobile worker roles and their enterprise information needs, including principally **Sales Personnel** (35% of mobile workers), **Mobile Executives** (24%), and **Field Service Engineers** (17%), as well as diverse groups such as military and government workers, health care providers, etc. (24%).

[1] Market metrics from Yankee Group reports.

The great number and variety of mobile workers means their collective information needs are as large and varied as workers within the enterprise, ranging from simple e-mail to critical data buried in enterprise applications such as ERP, CRM, etc. Analyzing next generation mobile enterprise markets, one market research firm concluded:

"The need for remote access to core company data and applications will drive adoption [of wireless data technology]. Success will be measured by the ability to efficiently link the back office to mobile devices so [mobile workers] have real-time access to customized, mission-critical data and applications." [2]

In turn, wireless carriers are eager to provide mobile data services because they are the carriers' principal future revenue growth opportunity. In the U.S., wireless voice services have become a commodity accompanied by aggressive pricing, shrinking per-minute revenues, and plateauing revenue growth. Current wireless data services (consumer and business text-based services) represent only about five percent of carrier industry total revenues, but even these limited services are growing faster and have better margins than voice services.

Nevertheless, this burgeoning demand for robust wireless data services is not being satisfied because of inherent constraints of wireless networks and challenges of enterprise implementation.

Constraints of Wireless Networks

Wireless data services depend on two distinct wireless networks to serve mobile workers. Because these networks do not interoperate and each has its own operating limitations, delivering the on-campus enterprise information environment is technically impossible, now and for the foreseeable future.

Traditional wireless carriers operate wide area (regional to national) cellular networks over licensed spectrum that can serve truly *mobile*, vehicular environments. Cellular bandwidth is narrow, a major obstacle for data services that even the very latest network technologies have no prospect of solving. For example:

- 2.5G packet networks currently being deployed have theoretical transmission speeds up to 144 Kbps but realized speeds are in the 40-60 Kbps range, about the same as dial-up.
- Prospective 3G and EV-DO networks may improve realized speeds up to 200 Kbps and 700 Kbps, respectively, still far short of what is necessary for robust enterprise data, and they will be expensive to deploy and will suffer from spotty coverage for decades.

In addition, because of the costs to license spectrum and to build out and maintain infrastructure across multiple geographic markets, service can be expensive for data that takes a long time to download. Moreover, cellular networks are designed for less than

[2] Frost & Sullivan

90% coverage reliability, so connections are frequently interrupted, thereby terminating any data transmission in progress and requiring a complete retransmission after service is restored.

The other wireless "network," WiFi, serves only local areas measured in feet, is more precisely *portable* rather than *mobile*, and consists of *individual spots* rather than *interoperating networks*. Services are cheap because WiFi operates over unlicensed (free) radio spectrum and there is no network infrastructure to build out, but viable business models depend on attracting incremental customers for the host's products and services (e.g., Starbucks, Hilton). WiFi bandwidth comfortably supports data transmission, but the strictly local reach doesn't serve mobile workers or communications with a distant enterprise.

Prospective new radio technologies such as WiMax and Mobile-Fi may compete to extend the range of wireless networking but still face the challenges of coverage and interoperability. As a result of these constraints, radio spectrum hotspots can only be part of a complete mobile data solution.

In short, there is no current or prospective network technology that offers a complete solution to the systemic limitations of wireless networks in providing mobile data services, including:

- Gaps in network coverage
- Less than 90% network reliability
- Slow data transmission speeds
- Lack of seamless interoperability

Any one of these deficiencies is a significant problem; collectively, they have been a severe obstacle. Moreover, some of these deficiencies are exacerbated during peak workday periods, when enterprise data is most needed by mobile workers.

Faced with these fundamental network limitations, current wireless data devices can only offer partial solutions with limited functionality that fall far short of ubiquitous sharing of the enterprise information environment. For example:

- Blackberry and Treo have good e-mail and instant messaging capabilities but are inadequate for working with large data files and complex e-mail attachments.
- Laptop radio cards are network-specific, require complex manual operation and special network-persistent technology (e.g., NetMotion), and only provide adequate speed where the service provider has upgraded its network.
- GoodLink only syncs selected enterprise data, without immediate access to up-to-date information.

Moreover, none of these piecemeal solutions adequately addresses the special challenges that corporations face in providing mobile workers with access to critical enterprise data.

Challenges of Mobile Data Security

Implementing mobile data services presents a severe challenge to protecting enterprise information because security of mobile access devices is minimal to non-existent. In the words of one analyst:

"Enterprises face potentially crippling loss if information such as personal communications, personnel records, customer data, and internal documents is inappropriately changed, accessed or stolen…Mobile devices represent a massive security risk…It is only a matter of time before these devices act as conduits for malicious and unauthorized access to enterprise assets."[3]

Moreover, enterprise security requirements are skyrocketing because of business-wide regulations such as Sarbanes-Oxley and because certain industries face special mandates for rigorous data security (e.g., HIPAA regulations for the healthcare industry). In addition, security challenges are compounded because certain information needs to be accessed by a changing cast of mobile non-employees (e.g., advisors, contract workers, vendors) as well as employees.

Safely extending the corporate information environment requires an *enterprise-grade* solution to security, so that enterprise information off-campus is at least as secure as it can be on-campus. Specifically, enterprise-grade security would incorporate:

- Authentication to ensure that (a) only authorized personnel can communicate on the network and have access to enterprise servers and (b) their access is limited to only those elements of information for which they have been pre-approved.
- Encryption of all information throughout its distribution off-campus.
- Protection against eavesdropping during transmission.
- Protection against unauthorized access to data after decryption.
- Tracking of which personnel receive what data, and from where and when the data is received.
- Protection against data being destroyed or lost after transmission off-campus.
- Central administrative control of mobile data services participation and infrastructure.
- Remote administrative ability to delete data after it leaves the enterprise campus.
- Perimeter protection against attacks through the enterprise firewall.

However, as critical as comprehensive security is, it is only one essential element of a true *enterprise-grade* wireless data solution.

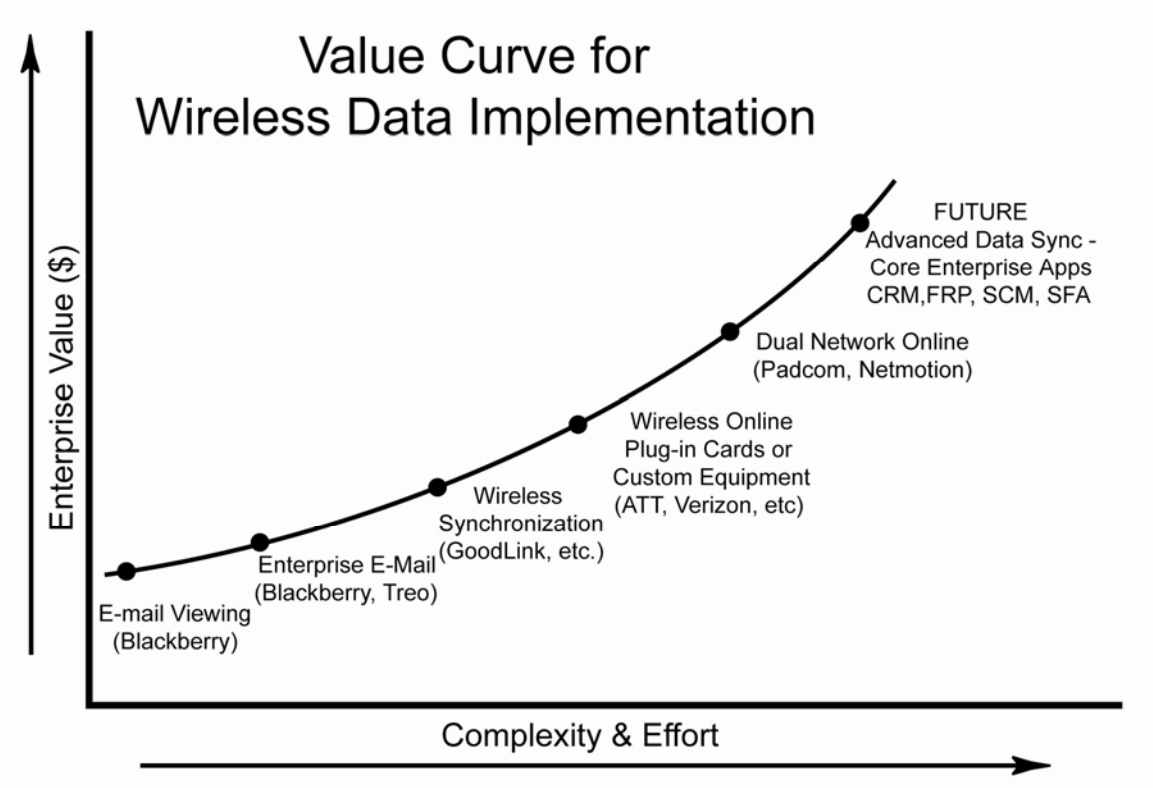
Other Corporate Challenges of Mobile Enterprise Information

In addition to security, implementing wireless data services presents enterprises with special technical and economic challenges not encountered with on-campus or voice services. In the words of one analyst, corporations want:

[3] IDC

> **"highly secure solutions available on multiple terminals at a low cost to implement and support across diverse user groups- a sweetspot the industry has been unable to hit."** [4]

Even simple text-based services put great pressure on already burdened IT organizations to support multiple users on multiple wireless networks using multiple devices such as notebooks, tablet PCs, PDAs and smartphones. And, as depicted in the following table, an enterprise confronts increasing complexity and effort trying to provision more complete wireless solutions for higher-value, more mission-critical data:



In addition to providing 100% security, a true *enterprise-grade* wireless data solution should be easy and affordable for businesses to implement no matter how varied the data, how large the mobile workforce, or how diverse the mobile device population.

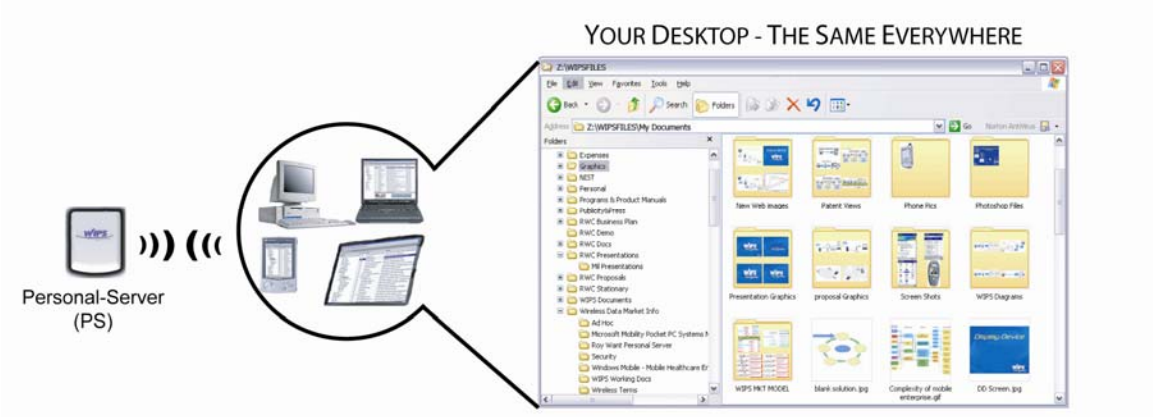
Thus, to really fulfill burgeoning demand for robust wireless data services requires an enterprise-grade solution that takes advantage of current and future wireless network capabilities without suffering from their limitations. The only such solution is WIPS, based on Rosetta-Wireless's Secure Mobile Enterprise platform.

The WIPS Solution

WIPS is the only complete, enterprise-grade wireless data solution that easily, securely and economically extends the enterprise information environment to mobile workers.

[4] Strategy Analytics

WIPS's breakthrough technology overcomes wireless network limitations by continuously *pre-positioning* current enterprise data to a wallet-size personal server (PS) that the mobile worker accesses with any mobile device, as depicted below:



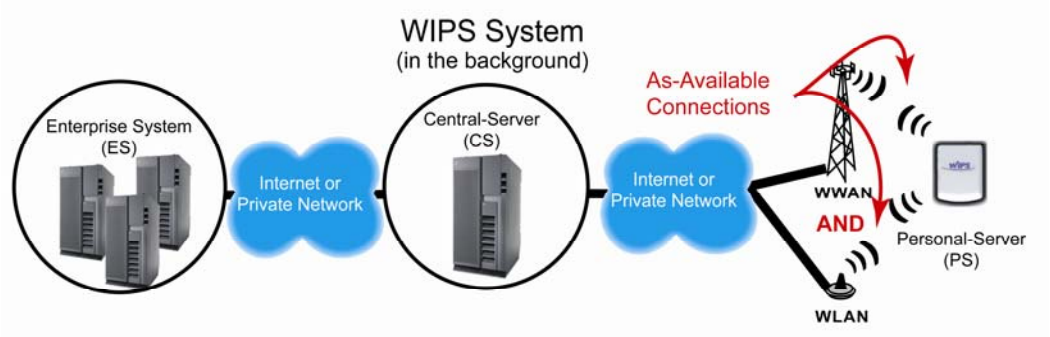
WIPS provides the mobile worker with an easy-to-use, flexible and totally secure information environment:

- The wallet-size PS has a battery life up to 16 hours and is easily carried in a pocket, briefcase or purse.
- The worker has immediate access to up to 80 Gigabytes of enterprise information identical to that available on-campus, including all data and applications such as:
  - Read/Write-to files stored on enterprise servers.
  - Enterprise Read-only files stored on file servers, including dynamically-updated files such as status and location of assets and personnel.
  - E-mail with *all* attachments and graphics.
- The worker uses any common mobile device (e.g., laptop, mobile phone, PDA) to instantly access and display the files stored on his PS.
- All data remains encrypted except when the worker is viewing or working with it and the decrypted data automatically disappears when the display device is turned off.

Moreover, WIPS operates automatically and continuously with no special user training required.

Design of Secure Mobile Enterprise System

The core of Rosetta's technology is proprietary communications software that links distributed hardware over established wireless networks into a wireless data platform designated the Secure Mobile Enterprise (SME) system. The diagram below shows the system design:



The SME system operates as follows:

- An intelligent, fixed-end Central-Server (CS) impersonates the mobile worker and continuously and automatically logs into the worker's Enterprise System (ES) through a single firewall access port. The CS is a standard computer in a single system or clustered configuration.
- The CS looks only at data, content and other files on the ES that the worker is allowed to access to identify those files that are new or have been changed since the last time the CS logged in. The CS then automatically encrypts and syncs those files to itself.
- The mobile worker's PS mirrors his files from the CS. The PS continuously, automatically and opportunistically completes wireless connections via available cellular (WWAN) and WiFi (W-LAN) access points. The CS and PS are logically identical, so that whatever data is on one migrates automatically to the other, remaining encrypted the entire time.

Rosetta's Secure Mobile Enterprise provides information security equivalent to what can be achieved on enterprise campuses. This is due to the SME architecture and because the on-campus system administrator retains control of both SME and information in the field. This security includes:

- End-to end encryption.
- End-to-end authentication because the PS and CS are logically paired and each system authenticates the other using a shared secret.
- Full access control to enterprise information because the mobile worker's PS communicates to the enterprise system only through an authenticated and secure CS.
- Complete data safety because of automatic duplication of all encrypted data so that if the PS has been lost or damaged, the data on the PS can be restored.
- Complete tracking of access to enterprise information, including who has received what data and from where and when it was sent.
- Complete system admin control over who receives what enterprise information.

- Full remote operational control over the mobile worker's PS from the system admin's console so that, for example, if the PS is lost or stolen, the system administrator can disable the PS by erasing (re-formatting) the PS hard drive and preventing the PS from reconnecting.

The Secure Mobile Enterprise system also is highly economical and reliable because:

- Except for Rosetta's proprietary software, it employs off-the-shelf hardware and software.
- It operates over existing wireless infrastructures and over any digital wireless network second generation or later.
- Transmission is on low-priority channels and during otherwise idle network moments, allowing exceptionally low cost services.
- Because files are opportunistically pre-positioned to the PS, the mobile worker has ready access even in the event of a dead-spot or system outage and has no wait for downloading.

In sum, Rosetta's WIPS and its Secure Mobile Enterprise platform provide a complete, enterprise-grade wireless data solution.

WIPS Features and Competitive Advantages

Unlike other wireless data technologies, WIPS is the complete solution, delivering enterprise information immediately, securely, and affordably, whenever and wherever needed. The following table summarizes WIPS's advantages compared to competitive wireless data devices and other technologies:

ATTRIBUTE / DEVICE	WIPS	Blackberry / Treo	GoodLink	2.5/3G Plug-in Card	Wireless Router	
Functionality						
Complete Replication of Enterprise Information	●		◗	●		
Instant Access	●	●	●			
Up-to-Date Information	●	●		●	●	
Ubiquitous Information Availability	●		●			
100% Secure	●		◗			
100% Session Persistence	●				●	
Features						
Compatible with Multiple Devices (Laptop, PDA...)	●		●	●	●	
Easy Operation	●					
Easy Scalability	●	●		●		
Cost	**Low**	**Low-Med**	**Med**	**Low**	**High**	

As shown, only WIPS is the complete, enterprise-grade solution to wireless data needs.

Carrier Business and Revenue Models

The first WIPS application is expected to be as a branded wireless carrier service offered under a license to WIPS software. The simplest carrier offering would be identical to current voice services for small and medium size business customers: the customer signs up for service billed on a monthly basis, receives a WIPS unit, self-provisions the service, and accesses his office server via dial- or log-in. (Either the carrier or Rosetta provide outsourced hosting of Central Servers.)

Rosetta management believes that a WIPS-based carrier data service could be priced below $100 per subscriber per month, which would be very competitive and also generate attractive margins for the carrier and Rosetta. Rosetta's revenues would be primarily in the form of license fees based on the number of wireless data customers.

Target launch for the first U.S. carrier service is 2005. This would be followed by licenses to other U.S. and to European carriers.

Other Wireless Data Markets

As a platform technology, Rosetta's Secure Mobile Enterprise system will enable "must-have" solutions for a broad range of mobile data services beyond that offered by wireless carriers. The common need is for *immediate, totally secure, and economical access to complete, up-to-date information from mass databases*. Major markets are expected to include:

- **Large Enterprise.** Needs are similar to those of carrier SMB customers, but likely to have special requirements as to scope of databases, security, etc.
- **Healthcare.** Healthcare providers need HIPAA-compliant access to patient information housed in diverse, independent databases such as doctor offices, hospitals, testing laboratories, pharmacies, etc. Rosetta's Secure Mobile Enterprise platform will be extended to communicate with these multiple systems and display information using provider-specific GUIs and devices, including charge capture for billing.
- **Homeland Security.** Comprehensive homeland security has security and multi-user needs similar to those of healthcare as well as the need to accommodate very large files such as images, maps, fingerprints, etc. Applications for Rosetta's SME platform are expected to aid in prevention, protection and defense against attacks, as well as in coping with and recovering from attacks. As one simple example, "first responders" to a crisis would have all the data and information they need, exactly when they need it.
- **Telematics.** Auto and truck makers are looking to wireless data technologies designed into vehicles for purposes of enhanced capabilities for communications, information services, security/safety, remote diagnostics/prognostics/monitoring, and entertainment. Rosetta's SME platform is expected to provide the essential communications functionality for all of these applications.

Each market will have its own business model, but it is expected that distribution will involve value-added resellers of Rosetta's technology such as system integrators. Also, the vast scope of opportunities suggests that Rosetta management may choose to license rights to individual vertical market segments to selected major U.S. and European partners.

Rosetta Background

Rosetta-Wireless Corporation was founded in 2000 and is headquartered in Oakbrook Terrace, Illinois. The Rosetta team is composed of veterans from such major communications industry, including such major firms as Motorola, AT&T, Ameritech, Bell Labs, Andrew, Lucent and Tellabs.

Rosetta's co-founder, CEO and President is Edward Bachner III, whose wireless background includes 20 years experience with Motorola. Rosetta's Advisory Board is led by Neil Cox, whose experience includes 20 years of executive positions with Ameritech and, most recently, Senior Consultant and Executive Vice President of Telecommunications Sector for Science Applications International Corporation (SAIC).

Rosetta's Secure Mobile Enterprise solution has been developed over a five year period. The development was accelerated in July, 2003, when Rosetta won a $2 million competitive grant from the Advanced Technology Program of the National Institute of Standards and Technology (NIST). These awards are granted only for technologies considered "revolutionary," "path-breaking" and that may potentially create "vast national economic benefits."

In August, 2000 and 2001, Rosetta filed patent applications in the U.S. and Europe, respectively, and significant follow-on applications have since been provisionally filed. Collectively, these patents afford significant proprietary protection.