



## FORMS AUTOMATION FOR THE GOVERNMENT INDUSTRY

### Streamlining Government Mobile Data Capture & Delivery with Turn Key Integration to Existing Host Systems

#### Issue

The issue of automating mobile personnel has been around for a decade or longer. Why then, if there are so many field automation solutions, are so many field employees still using paper, driving the paper back to an office and entering data manually into legacy systems, or struggling with their cellular data coverage to send these large data files? While field force automation is not a new topic or problem facing the fed/state/and local governments they are still struggling to:

- ✓ Deploy the right mobile platforms that are easy to use, easy to deploy, and easy to maintain.
- ✓ Integrate data captured in the field to legacy systems without the need for large IT resources and expense.
- ✓ Solve cellular data coverage issues that prevents field users from reliably sending and receiving data files.
- ✓ Provide adequate security levels at all layers.

#### Background

The definition of a successful field automation solution is one that is easily and widely adopted by mobile workers, is flexible to both IT and field personnel, allows data captured remotely to be easily sent to where it needs to go and does not require massive IT resources to build, deploy and maintain. If the above is achieved, The Gartner Group estimates enterprise ROI averages, reflecting real dollars saved and productivity enhancements over total cost of ownership, range from 300%-700%.

Government agencies at all levels are learning how to improve responsiveness, manage assets more efficiently, decrease capital expenditures, use greener technology and reduce labor requirements by adapting mobile and wireless technologies that are used extensively in the private sector. The main building blocks for automating field operations are a **mobile hardware platform, wireless & host system connectivity, application software, and security** to make it all run smoothly.

## ***Mobile Hardware Platform***

Mobile computers must be matched to their usage conditions to provide reliable performance and ongoing value. Some important selection criteria include whether the device will be used indoors or out, ruggedness, the preferred software operating system, screen size, memory, available card slots and interface ports, support for desired input method (e.g. touchscreen, keyboard entry, forms-based pen computing,) and support for desired wireless connectivity and security.

Like most computer devices there are constant trade offs between cost and performance. The single most important thing to remember in driving ROI in your selection of your mobile platform is...."Can the field professionals use the device comfortably and will they be more productive"? Procurement might find a "great deal" or non-field users might prefer certain operating characteristics but if the people in the field don't find the device useful in performing their daily functions, the automation solution will fail!

## ***Wireless & Host Connectivity***

Broadband wireless data cards are widely available from cellular carriers and can easily be embedded or plugged into laptops, tablet PC's or other mobile computing devices. Broadband connectivity is also widely available in PDA and smart phone devices. So what is the problem? Several potential pitfalls in deploying mobile workforce solutions were highlighted at the Gartner Group's 2007 Wireless Summit. Among the potential critical planning errors were:

- ✓ **An over reliance on the pervasiveness or ubiquity of broadband wireless data networks.**
- ✓ **Assuming your field workers will have access to the Internet for Web based solutions.**
- ✓ **Assuming your field workforce can retrieve and send information over a VPN.**
- ✓ **Failing to recognize the lack of wireless security when using commercial wireless data networks.**

There is a real need for a persistent, intelligent, managed communications layer between your field users and the Internet, your VPN and your backend systems. Such a systems managed (as opposed to field user-managed) communications layer can provide wireless security, guaranteed delivery of your data to its final destination and give the field user a positive experience. Such a communications system also allows for a reliable "push solution" for sending data, updates, new forms, etc. directly to the field device without requiring initiative by field personnel.

## ***Application Software***

It sometimes seems there are more software choices for automating field processes than there are field processes. Unfortunately, the vast majority of application software choices are not focused on the end to end needs of field automation—namely easily and accurately collecting the needed field data, promptly and securely delivering the field data and seamlessly integrating that field data into host systems—many times multiple host systems.

Many of the available application software solutions tend to be narrowly focused on specific field tasks and requires the field user to manage (find) the necessary connectivity to transmit the data. The biggest deficiencies in field automation software solutions today that have directly lead to slow and/or delayed adoption are:

- ✓ **The User Interface (GUI) is not designed for use by field workers.**
- ✓ **It can typically take 3 iterations to get the user interface (GUI) while everything continues to back up.**
- ✓ **The solution is not matched to the varied skill sets of the field personnel and the solution requires more than a relatively low level of training because it is not intuitive and “easy” for the field user.**
- ✓ **Difficulty in seamlessly managing the delivery and integration of mobile data into numerous and varying back end host systems. (This is a critical element in unlocking the full ROI of the solution but can be costly and consume vast IT resources and dollars if not managed properly).**
- ✓ **Selecting as much “off the shelf” software as possible to eliminate the need for custom code instead of choosing software that quickly and efficiently deposits mobile data into multiple legacy systems without significant IT effort.**

## ***Security***

Field2Base has recognized the requirements for security mechanisms and controls at all layers of the solution. Here, we will briefly discuss securing agency data at the physical (mobile hardware), software, and transport layers for the Field2Base solution.

- ✓ **The Field2Base thin client can be located on any laptop PC, tablet PC, UMPC or Netbook running Windows XP or Vista operating system and any PDA device using Windows Mobile 6.1 operating system or newer. These platforms allow for the use of stringent software and hardware security options (biometric, magnetic swipe, etc) which ensure the device is locked until user authenticity is validated.**

- ✓ Each form generated and sent by the end user is placed into a 256 bit AES encrypted digital envelope for transmission. The envelope is not decrypted until inside the agency firewall (DMZ). The default for the application is to retain a version of the data in the encrypted envelope inside the client. This allows for saving work as drafts or to resend information if necessary. If at any time, the device is lost or stolen, an administrator can send a “kill pill” to the device and remotely destroy access to the data on the hardware.
- ✓ Federal agencies should maintain the Field2Base server software in a DMZ behind a FIPS 140-2 compliant SSL VPN or other FIPS certified appliance. Any information traveling from the Field2Base client to the Field2Base server is secured using 2-factor encryption. The data packet itself is encrypted using a 256 bit AES algorithm and is then encapsulated in an SSL tunnel created by the VPN appliance. At **NO POINT** during the transmission from the client to the server is the data visible to a third party.
- ✓ Federal Agencies also have the ability to Manage / Track their workers and assets using real time GPS reporting the Field2Base module, MyWorkforce™.

### **Conclusion and Recommendations**

When evaluating field and paper automation projects, government agencies need to focus on the end to end process—data collection, data delivery and data integration—and select devices, technologies and software that provide enterprise capabilities that address each key element of the total solution. Data collection devices must not only be capable of performing required enterprise tasks but also enable all field users, regardless of skill level, to have similar and easy field experiences.

By using mobile computers and supporting technologies, organizations can eliminate the errors, delays and clerical costs associated with recording information on paper forms and the additional step of keying the data into a computer system. With the right mobile platform and automated data entry, information is entered in the field where the data is originally captured and checked for accuracy before it is forwarded to the host computer system **ONE TIME**. This information, now in a digital format, not only contains the text data that was previously being captured but can also include enhanced media such as: photos, barcodes, signatures, annotations, GPS information and biometric information among others. Wireless communication technologies together with a progressive software solution enable field information to be exchanged in real-time across any distance or location.

Commercial systems, such as the Enterprise Suite from Field2Base® combined with the right mobile hardware platform (Tablet PCs, laptops or handhelds), provides the necessary user experience, managed, secure wireless communications and data integration tools that enable Agencies to reap the substantial benefits of “Going Green” by deploying paper automation solution.

\* Gartner Group, 2007 Wireless Summit