



## FORMS AUTOMATION FOR THE GOVERNMENT INDUSTRY

### **Solution Security Overview**

#### **Overview**

Field2Base is a mobile data capture and delivery (e.g. forms automation) solution for Federal Agencies. The solution delivers real time form data from the field to existing host systems using a FIPS 140-2 certified architecture. In this brief white paper, we will discuss securing agency data at the Physical (Mobile Hardware), Software and Transport layers for the Field2Base solution.

#### **Physical Mobile Hardware Platform Security**

The Field2Base thin client can be located on any device running Windows XP or Vista operating systems (Laptops and Tablet PC's) as well as any PDA device using Windows Mobile 6.1 operating system and higher. Most hardware platforms offer stringent security options (Biometric, Magnetic Swipe, Etc). Devices such as biometric fingerprint scanners keep the device locked until user authenticity has been validated.

Additionally, the Microsoft platform affords IT personnel significant opportunities for deploying third party applications which may be used to secure the device. Device security is paramount to protect sensitive information contained within Field2Base and all other local applications should device become lost or stolen.

#### **Field2Base Software Security**

Each Form (or other piece of mobile data) generated and sent by the end user while using the Field2Base client is placed into a 256 Bit AES encrypted digital envelope for transmission. This envelope is not decrypted until inside the agency firewall (DMZ). The default for the application is to also retain a version of that data, in the 256 Bit AES encrypted envelope, inside the Field2Base client. This allows field personnel to save work as drafts or resend information if necessary.

If at any time, the hardware is lost or stolen, the Field2base administrator can send a "kill pill" to the device and remotely destroy any access to the data created within the Field2Base client located on the hardware. At no point, during either transmission or retention, is the Field2Base digital envelope decrypted, until it is delivered to the agency secure environment, where the agency will be hosting the Field2Base server. The Field2Base client application also has a password protected login feature if desired as an additional level of security at the end user level.

## Data Transport Security

Federal Agencies will maintain the Field2Base server in a DMZ behind a FIPS 140-2 compliant SSL VPN or other FIPS certified appliance (**See Figure 1A**). Any information traveling from the Field2base client to the Field2Base server is secured using two- factor encryption. The data packet itself is encrypted using a 256 Bit AES algorithm from Field2base and is then encapsulated in an SSL tunnel created by the VPN appliance. At NO POINT during the transmission from the Field2Base Client to the Field2Base Server is the data visible to a third party.

