THE NEED

Asian consumer goods manufacturers transfer goods to distributors in different regions. These distributors are then responsible for sale of these products to various retail outfits through delivery personnel. Sales and delivery personnel deliver goods to the retailers, collect cash and receive orders for the next delivery. Data entry is typically on paper. The paperwork and cash collected is handed over to the distributor to reconcile cash received with goods delivered.

In contrast, the field force abroad enters information into electronic forms displayed on handheld devices, as opposed to paper forms that later need to be converted manually to an electronic format. Manual data entry and book keeping functions are thus eliminated. Providing mobile connectivity at the field level results in:

- Increased sales by providing better sales forecasting based on timely and accurate field data.
- Better decision support tools, available on the hand held, for the sales person in the field
- Instant access to sales history and retailer information, available on the hand held
- Reduced loss of sales stemming from stock outs, due to inaccurate sales or delivery information
- Reduced distribution costs, by eliminating tedious book keeping, previously performed manually.

A large consumer goods manufacturer in Asia manages, through agents, thousands of warehouses or depots, each of which maintain 10-50 sales and delivery persons to deliver goods and book orders. Additionally, there are company sales persons working the field gathering market intelligence.

Enterprises are aware that the field level is the bottleneck in their otherwise efficient sales and distribution chain. But implementing mobile device connectivity have failed: Palm based solutions are too expensive and impractical in Asia's harsh environment. Nor do they provide a complete solution involving data flow into the enterprise and security concerns.

CURRENT SITUATION

In fact nobody even wants a computer. What everybody wants is that magical toy that can be used to browse the web, balance the checkbook and so on. The fact that you need a computer and an operating system to do all this is something that most people would rather not even think about.

Linus Torvald, in "Just for Fun: The story of an accidental revolutionary"

- SERVER CENTRIC AS OPPOSED TO CLIENT SIDE COMPUTING
- INTERFACE DRIVEN AT CLIENT SIDE, APPLICATONS RUN AT SERVER SIDE

The Thin Client Model

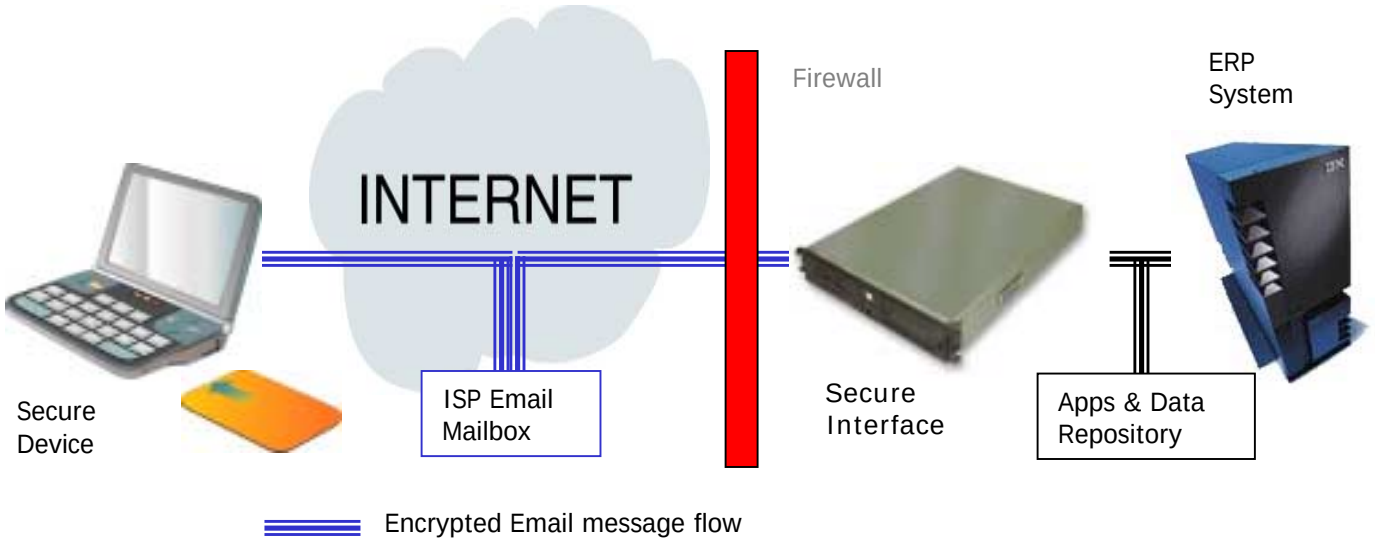
The thin client model of computing has emerged as the low cost solution to connecting all nodes of the enterprise. As the term thin client suggests, the bulk of the computing is transferred to the server side. The local computer or handheld device is effectively a remote terminal, or client, to the server application. A common example of a thin client is the web

browser that displays “forms” transmitted from a web server. While elegant in concept, thin client solutions assume that web servers are accessible at any time or place. Therein lies the problem of implementing such solutions in Asia.

INTERMITTENT CONNECTIVITY

A thin client approach for Asia must address four issues:

- Low Device Cost — Providing low cost thin client device to collect and transfer data in an electronic format
- Secure & Robust — Providing secure robust Internet connectivity all the way down to the thin devices.
- Simplicity of Use — The operation must be idiot proof and remotely controllable – like a web browser.
- Extend not modify — Solution must integrate with the existing ERP framework with minimal modifications



Using secure email as the medium to provide thin client solutions

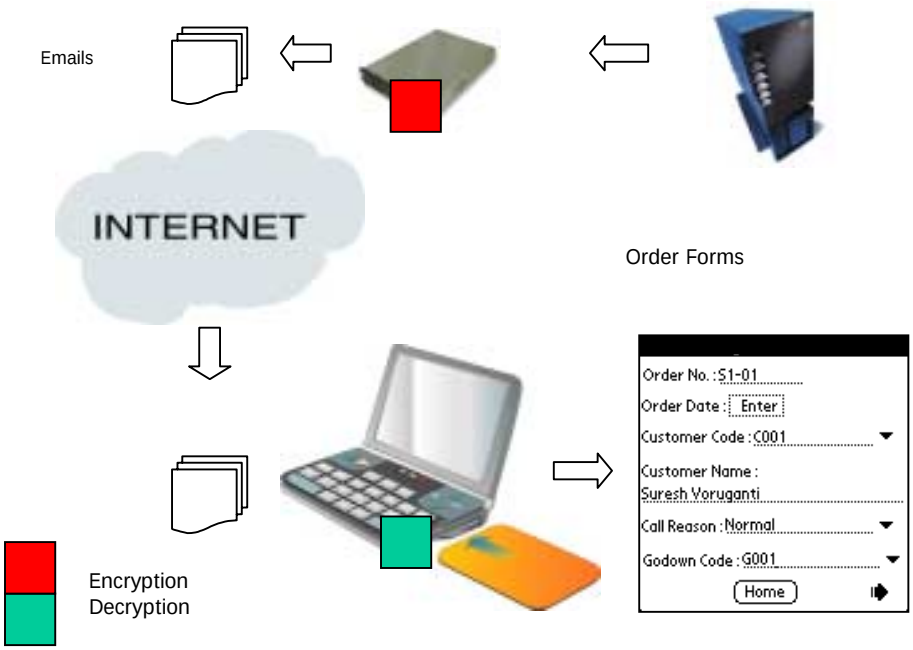
A paradigm shift is needed - from thin client “thick” connectivity approaches to specialized thin client like devices designed for “thin” connectivity.

The field force needs to communicate with the enterprise on a periodic basis, typically once a day. An intermittent connectivity model using email, for example, is a viable option. Extend the concept of email to include sending forms and receiving back data from filled forms, and we have the beginnings of a workable thin client approach – based on intermittent connectivity.

In concept, a new type of low cost handheld devices could act like a disconnected browser. It would receive forms to be filled in the field, and later, at the end of the day, return the responses to the “servers” that sent the forms. A thin client in concept, these thin devices provide periodic connectivity with the enterprise, in situations where constant online accessibility is not practical or necessary.

Paradigm Shift: From thin clients designed for thick connectivity to thin devices designed for thin connectivity.

EMAIL BASED THIN DEVICES



A thin client approach based on email

Conceptually a email based solution could be implemented as follows:

- Send an email from the server to the email account of the thin device.
- Include in that email forms that need to filled and returned, just as online forms in would be filled and sent back.
- When the device logs on to the local Internet Service Provider (ISP), the emails are downloaded to the device.
- The device "reads" the email and displays the forms to be filled in the field
- The Field personnel fill out the forms in the field.
- At the end of the day, the forms are converted to email messages and sent by email to the enterprise.
- Software at the enterprise, "reads" the email, extracts the data needed and runs bookkeeping applications.
- The cycle repeats.

The emails sent to the device could include applications that display a set of forms that need to be filled according to a predefined sequence. Later, a validation check may be performed by the application so that data sent back is clean. This is similar in process to having data entered on a web page checked by scripts inside the web page.

Virtues of an email-based approach to send and receive data in this disconnected manner are:

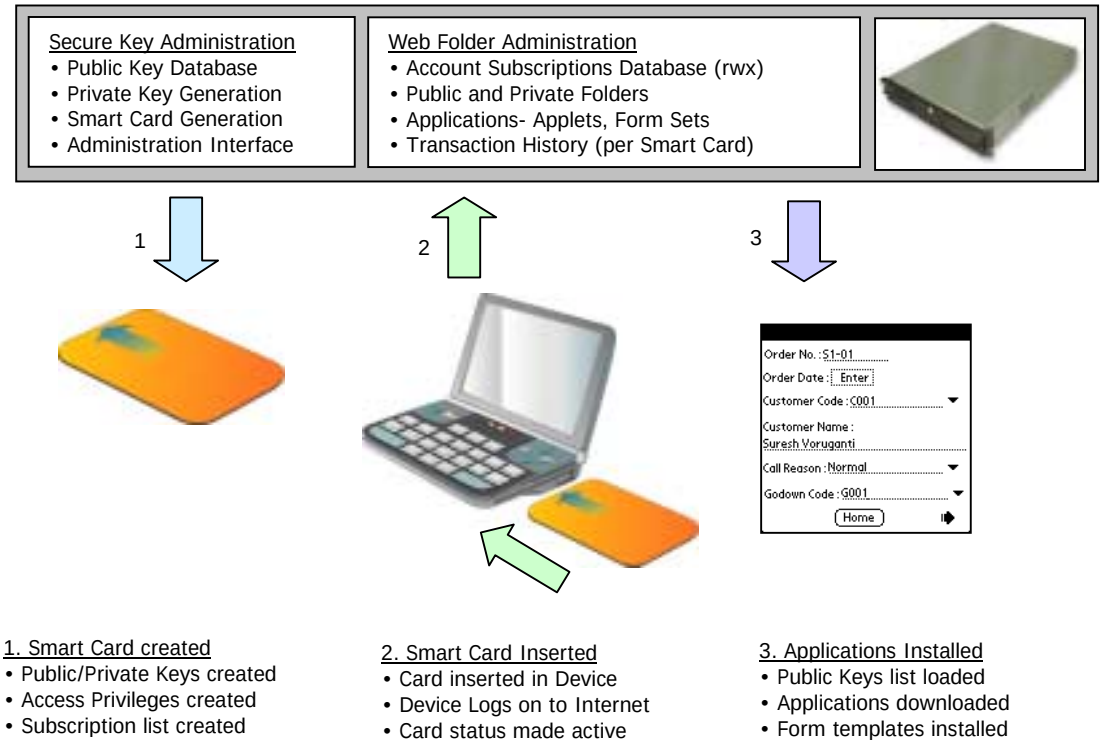
Robust Message Delivery Email is stored in a mailbox till picked up. In the event of a device failure, the email remains in the mailbox. Email may be removed from the mailbox only after the transmission is complete – that is the email was sent, received and the response transmitted. Additionally, a copy of every transmission can be maintained in another mailbox, should a transaction history be needed.

Point to Point addressing. You cannot get an email not addressed to you. Even if you "steal" the name and password of a friend's account, there can be other security measures (discussed later) to ensure that you and only you can access your email.

No exposed Interfaces. Hackers break into systems through exposed interfaces – such as web servers or FTP servers. Email based message delivery is not an exposed service – the outside world cannot access it the same way they can access a web server, resulting in a higher level of security.

Approach: Use Email as a thin connectivity medium. Provide devices using email to implement thin client solutions.

REMOTE MANAGEMENT OF DEVICE



Remote Management of Device

A thin client approach eliminates application deployment in the field by maintaining the applications in the central server with no applications permanently loaded on the device. Conversely, intermittent connectivity situations, using email, require some part of the application – usually data entry and validation - to reside on the device. For the email approach to work, "field" applications must be installed and updated through some automated means that can be managed remotely - and securely - by the enterprise.

Security is assured through a variation of the Public Key Infrastructure (PKI) approach. Two keys, one public, the other private, are used to encrypt and decrypt messages sent over the Internet. The Public key is freely available to anyone encrypting messages intended for the owner of the key. Only the secret private key can decode the encrypted message. The power of this approach is that it does not require "trust" or sharing of the private key.

In our approach, public and private keys are supplied by distributing them on smart cards. When the smart card is first inserted in the device, the device logs on to the local ISP and sends an email, containing the public key to the enterprise. In much the same manner that a cell phone is activated, the smart card is then activated at the enterprise end as a bona fide member of the distribution chain:

- The public key sent from the card is registered in the database as "active"
- Applications intended for that user are sent to the device's email account.
- A public key list needed by the user (to deliver secure messages) is sent.

The next time the device logs on, email attachments are transferred and appropriate folders on the device updated. The device can now receive secure email, encrypted by the public key on the smart card now available to enterprise. The secure mail is decrypted using the private key on the smart card. Remove the smart card and no access to the secure messages is possible. As an analogy, a cell phone is useless without the SIM card.

Remote administration of the device is also handled through secure emails. Emails authorizing changes – such as deletion of public keys, in case of stolen cards - are recognized only if they are signed employing a digital signing method, also based on the Public/Private key system. Remote secure management of the device is now feasible.

A complete solution: thin devices, software applications and a security infrastructure all working together

ABOUT ACG

Advanced Cybernetics Group, Inc. (ACG), incorporated in 1992, develops software for high performance embedded systems. Self-funded development has resulted in products sold to IBM, Schlage Lock, Adept Technology, Motorola and Seagate. We are an approved Department of Defense supplier. ACG is based in Silicon Valley, with offshore development teams in India. Visit us at www.advancedcybernetics.com.