| Industry Problem | Communication Solution | Lessons Learned |
|---|---|---|
| Retail-Inventory control and lost packages | RFID | + Enables communication 24/7<br>+ provides automated continuous tracking<br>+ Reliability<br>-$.30/ea. Makes cost prohibitive<br>-data can be lost if chip damaged<br>-cost of scanners |
| | | |
| | | |
| | | |
| | | |
| Interactive data input | HTTPs | + Ease of implementation<br>+ Ease of management<br>+ Very standard<br>- Some additional overhead and minimum loss of throughput |
| Document exchange | AS2 | + Flexible - can handle multiple message types<br>+ Designed to push data securely and reliably over the Internet<br>+ Fast and reliable connectivity<br>+ Encryption ensures that only the sender and receiver can view the data<br>+ Digital signatures ensure authentication: only messages from authorized senders are accepted<br>+ hash algorithm detects if the document was altered during transmission<br>+ receipts for delivery<br>- Certificate management |
| Document exchange | FTPS | + Well known standard<br>+ Delivers strong authentication<br>+ Provides confidentiality on both the control and data channels<br>+ Ease of implementation and training<br>+ Flexibility to use either SSL or TLS<br>- Potential firewall complications<br>- Certificate management |
| Document exchange | SFTP – SSH-2 protocol only | + Reduces certificate management requirements<br>+ Flexibility in managing the “remote” files<br>+ Clean resumption of interrupted transfers<br>- Found limited understanding across the community (more training and discussion time required with our partners)<br>- Protocol is not yet an industry standard |

| | | |
|---|---|---|
| {Mobile phones} Remote deployment, management, and provisioning of consumer devices (mobile phones in wireless networks) | Multiple layers:<br>• The consumer device is "locked down" to contain malicious consumer behaviors.<br>• The network forces the device to authenticate before granting access to services. | • Assume that devices are intrinsically not trusted and untrustworthy<br>• Conduct all security / authentication features transparently from user<br>• Consumers claim to want high security features, yet few of them are willing to put up with the incremental costs (time, hassle) required when actively implementing those features. |
| | | |
| | | |
| | | |
| | | |
| | | |
| Banking-Efficient routing of manual transactions | MICR encoding | - Hub and spoke requirement for national coverage (Federal Reserve branch model)<br>- Mandatory standards participation<br>-Physical transportation challenges (ie. Inclement weather, 9/11, etc.) build exposure and risk |
| Real time global transaction processing | Mag Stripe card and PIN | - Limit funds availablility to minimize exposure<br>- Interconnected switches required to link multiple card bases<br>- Difficulty linking users to PINs |
| Real time global transaction processing | Smart card (EMV) and PIN | - Added security lowers risk profile<br>- 10x cost vs. mag stripe<br>- Ability to support biometrics |
| | | |
| | | |
| | | |
| | | |