ROI Comparison For Embedded Biometric

ROI Highlights

- Finger/Template Only System
- Embedded Software At Device (Edge Device)
- Remote Access / System Management Over WEB
- No Servers Or Backshop Computers Needed
- Browser Infrastructure
- Reader w/Keypad Environmentally Enclosed (Interior/Exterior use)
- WEB Access Behind Firewall Or Remotely Through VPN
- Base Component MSRP Roughly $2400 First Door & $600 Second Door
- 96 Door Capability For Non-Enterprise System
- Enterprise Management Available – Unlimited Doors
- LDap Through SAP Available
- Multimodal Biometric Available

As Vice President of Security for a major Financial Corporation located in California I was privileged to review many thousands of products in my history with that company. The last major program I managed began as a $40,000,000 key control project that would have affected 4500 locations and netted the collection of half a million keys. The project, using smartcards, is actually a success in many ways. It lacked however an effective ROI. And an immediate return (in large dollars) could not be shown after completion. For this reason the project scope was narrowed to only a single state.

A change in project scope due to ROI is not an isolated case as I have seen many projects affecting all types of industries change direction on major access control projects, specifically merging physical access. This paper is intended to clarify the operation and infrastructure requirements of Enterprise systems as well as state comparisons for mid-size and local systems. The objective is to identify how cost centers that support such systems can be methodically reduced and controlled.

For the record the product used for comparison is relatively new on the market (for the last three years) and manufactured by e-Data (www.e-data.com). e-Data has requested this paper to clarify discussion on cost points when comparing their product to other providers/systems. In this discussion I will be drawing on my experience not only in the Financial Industry, but also Government Programs and Commercial Programs that I have witnessed or been directly involved in. For this ROI discussion we will take each element separately building to the Enterprise level.

Small System Design: Why Embedded software? The way the major Access Control systems are designed today (though they are moving in the embedded direction) is to require a Controller, having full functionality with data base and requiring remote software to manage it. This may not sound like much but the average controller is $2,500-$8,000 in cost depending on the number of doors it manages (8, 16 or more). The cost of readers and various other features that are hung on it would be additional. Remote software for small systems runs $5,000 to $10,000 or more based on the number of controls reporting to it. This does not include the price or the server ($3,500-$25,000 each) or it's back-up counter part, with terminals to house the software. True many major systems are now incorporating VM or virtual capability to reduce server costs, but at this point dedicated servers are still recommended. So if we are conservative and add up the numbers: A controller is $3,500 (four door capacity), Each reader is $600 ($2400 total for four doors), Management Software is $8,000. A small four door system (locks, cable, install would be similar to all systems for this discussion) would cost roughly $14,000. An embedded system would be half that amount. The savings is in management software. Embedded systems contain the management software in the device.

Did I mention cards? Let's say that we have the need for 2000 cards (a population of roughly 1000 workers). At a minimal price with programming and shipment for standard 13.5MHz/125KHz proximity the price would be $5/card or $10,000). If we are using biometrics as the e-Data product provides, this overhead goes away. So far we've saved $17,000 on this installation through the use of embedded biometric product and I have yet to mention the badging equipment and personnel to manage the process (our savings could be $50,000 or more if administrative fees are added, see card discussion below). The question can now be asked: Are badges necessary in a world without cards? Some would argue "yes" but I would state that credentials should be used only in high security areas. In many organizations the badge is not worn but retained for access control. If the latter is the case the badge is not needed. If badges are required for identification, then inexpensive cards (PVC) would do at $.05 a badge.

An organization such as the one above with 1000 workers will have need of personnel to badge new employees, process badge returns, issue temporary badges, etc. The full time staff required may be one or two individuals. When there are no badges to process, there is only the enrollment of new employees or deletions of former employees to contend with. System management for this company could be a part-time function.

Enterprise Systems: Consider the scope of an Enterprise system: It may contain anywhere from 500 to 10000 readers applied to both perimeter and interior doors; The number of employees may be as few as 10000 or as high 500000 spread across the America's, Europe and Asia. Hardware used for an Enterprise system would follow that laid out for our small access system described above, but with some very important differences. Many Enterprise systems in use today are made up of amalgamations of many systems of varying types/size acquired through the growth of the company. This means that readers, cards, controllers, management software and the servers that house it are discrete in operation. All components in an Enterprise system are dissimilar and all are based on card technology. There are a few companies that have a completely uniform access control system, but they are the exception. The rule being that the higher the degree of dissimilarity of access components the higher the costs for system operation. The cost centers where savings can be identified are: Service license fees (that range from $15,000 to $50,000 per year per server/site, twenty servers in a system is not uncommon); Full time employees that number from five to twenty for 24/7 supervision ($500,000 - $1.5 million/year); Enterprise management software that bring all discrete access systems under central control ($50,000 - $350,000, with a yearly license of $20,000 - $50,000); The HR interface for Enterprise notification of employee termination ($100,000 - $350,000, with yearly license fees of $20,000 - $50,000/year); Lastly the raised floor space for server operation ($250,000 - $1,000,000 annually). Are these costs clearly visible to the Enterprise? Perhaps, but if several departments share any portion of them the reporting will not be to a single cost center.

A uniform biometric platform such as the e-Data product may reduce these cost in several ways. Servers and license fees would be cut substantially, thereby reducing the need for data center (raised floor) space. Enterprise management software for discrete systems, with its recurring fee would not be required. With a uniform system the HR interface software would not be needed. While this may seem contrary to established industry practice, it actually appears to be the simplest solution on an Enterprise scale for access control operations. Taking the midpoint costs in our example a full conversion to a biometric platform may cut $2,000,000 in operations expense. To underscore this statement we need only look to the actual cost of the access card to see that our statement of savings is quite reasonable.

Actual Cost Of Cards: And what is the real cost of cards to the Enterprise? For our illustration we will use 100,000 workers that require 125,000 cards. Most everyone is phasing out their 125KHz proximity cards and moving to smart 13.5MHz technology. But the price of either card is not what you see on paper. The base cost could be as low as $5, but programming and printing will add another $10 or so to the card. Then there are the “soft” costs (the infrastructure costs described above) for management, processing and administration that are added on by the department handling the card. These soft costs are simply passed through to the user. In 2003 the price stated by one corporation was $45/card to the business unit. Replacement costs for a 125KHz have been at $25/card for years. So the actual cost of a card with handling (internal/external) is anywhere between $25 and $65 per card. The price for a Government TWIC card is reported to be $125. If we use a conservative figure of $45/card surely the business unit that gets the bill must be asking themselves what value besides physical access am I getting for this price. If the card costs are covered by enhance operations, such as single sign on or logical access, or machine identification, then the program benefits may provide returns that cover these costs. The returns from the enhanced operations should be immediate and not future based otherwise the $45/card cost can not be reasonably justified. The actual costs of 125000 cards in this example would be $5,600,000. It is clear from our discussion that the Enterprise should be able to recover a major portion of this cost. It can do this through the application of a uniform biometric product which will reduce management overhead and remove the use of cards.

Having laid the foundation for this cost analysis we must remember that any Enterprise of any size will move slowly to adapt new technology and affect its infrastructure. The process would begin with new project construction and to the areas where the highest cost savings can be made. Card systems and biometric product such as e-Data’s could remain side by side as long as the card system was efficient and cost little to operate.

Suggested Application:

Key Management - Key control is a hot compliance issue at this time. It's well known that keys are difficult at best to manage but now Audit and Compliance changes have made it mandatory to know where every key is. This in many cases is not possible. The average dollar amount for key replacement ranges from $500 to $1500 annually just for the perimeter door (main entry). The costs for reconciling lost keys or responding to audit reports may be $2000 annually. If there is fast turnover then the numbers are much higher. The application of biometric access control would result in a return on investment within the first year of operation for a company with normal key maintenance.

Teller/Cash Drawers - Fraud losses at a small bank can be as high as $10,000,000 per year. It is estimated that 30% of that loss amount is from internal theft. One bank that applied biometric controls to their teller line reported nearly zero loss. In a large store there could be as many as twenty registers. In a bank at least ten cash drawers. Key controls are a major concern here. A biometric device on the teller bus or register would insure that only that teller at that time entered the cash drawer. Not all losses can be brought down to zero through biometrics however it should speed the investigation and management of those losses. And will act as a positive deterrent.

Cash Rooms/Containers – Biometric access through e-Data's product can be applied to safes and cash processing rooms, such those found within markets ("Instore Banks") to control access to the room as well as the cash container. The application is well suited to ATM rooms and the machine chest, where servicing is done by employees. Also for day storage safes, where access to cash must be quickly made. Where there is a large merchant population with resulting deposit claims, a biometric reader on the night deposit would solve those issues quickly and allow deposits to be easily traced. A word to National ATM service contractors: The e-Data product would speed access for replenishment personnel replacing the need for room key, token updates or combinations. ATM room and machine alarms would be deactivated automatically, saving time and the costs of fines/fees on false alarms.

Communication Rooms - Data and communication rooms have always been an issue with most corporations. Access, especially after-hours and deactivation of alarms (if they have them) are the main items for concern. As the e-Data product allows for deactivation of alarms and remote PIN application, access issues would be resolved, the rooms would remain fully secure and the compliance/Audit issues that have been nagging the company for years would be gone.

Summary: The e-Data product review found it to be impressive in design, management and cost effective. A world without access cards and badges is hard to imagine. e-Data has made it possible to think in these terms. At minimum the product allows existing card systems to have biometric options that run in parallel with standard card operations at a significantly lower cost than building a biometric system based on card technology. The industry has been searching for a cost effective business model for the biometric enrollment of 100,000 employees on an access system. The e-Data product may be it. I certainly recommend a thorough examination of it.