

CHOOSING AN OPTICAL MEMORY CARD: AN APPLES AND BANANAS COMPARISON

By Bruce Kelton, Keltec and Andy Rushworth, PeopleCount

TURNKEY SYSTEMS AND INFRASTRUCTURE SOLUTIONS ENDEMICALLY INCLUDE RISK ANALYSIS OUTCOMES, SECURITY CONTROLS AND THE CONTROL AND USE OF BIOMETRICS, NON-REPUDIATION AND AUTHENTICATION PRINCIPLES AND TECHNIQUES. BUT WHAT ARE WE TRYING TO ACHIEVE HERE, AND WHAT IS THE RISK OF FOCUSING TOO NARROWLY, TOO SOON? DOES TECHNOLOGY REALLY HAVE ALL OF THE ANSWERS? AND WHAT DOES A BANANA HAVE TO DO WITH THIS?

Since 9/11, technology has received increased funding to meet operational requirements. Focus must now be placed on ensuring the delivery of working and enduring solutions. Can hardware providers also provide the business intelligence to implement solutions into an enterprise process model? They may have the capability to create and store a biometric, but how do you manage and securely deliver a database of 18 million of them? For instance, the largest databases built today are in the banking sector, where signature images in excess of 17 million are used for verification and identification.

Technology alone does not have all of the answers, particularly when it comes to non-repudiation and the protection of privacy when applied to a transaction that includes a biometric. So what does common sense dictate about the use of these technologies?

RISK ANALYSIS

A risk analysis should support the answer to this question and enable identification of any failings.

- Protection and security almost always involve additional expense, but should always be justified in risk financing terms.
- Confidentiality, integrity and availability are basic principles that should be applied across the enterprise, and not just restricted to IT.
- Security should be properly targeted and directly related to potential impacts, threats and existing vulnerabilities.

A business risk analysis should also embrace those systems not under the direct control of IT, such as paper-based systems, systems using other office equipment and access control. The analysis should include the identification of necessary control, procedural and policy statements. IT can further define technology and project risk. The process should enable security to be driven



Technology alone does not have all of the answers, particularly when it comes to non-repudiation and the protection of privacy when applied to a transaction that includes a biometric



into more areas of the enterprise, becoming devolved and endemic throughout. ExxonMobil do this very well.

Risk is high where no definable best business practices, business risk assessment and accountability exist. Where established controls, policies and procedures are written down and followed, risk is decreased. When these controls and procedures are sacrificed, prudence is the next best approach and is usually resorted to when no regulation or best business practices exist. Due diligence – another legal word – requires that an enterprise meet federal regulations, use best practices and be reasonable and prudent in its dealings. An enterprise that fails to meet these criteria leaves itself open to litigation and failure if it doesn't respond appropriately. Recent examples of this failure are, amongst others, HIH and OneTel.

OMC: INTRODUCING THE BANANA

We all know the apples-to-apples comparison: we buy whichever apple is cheapest. For this scenario, think of smart cards as apples. Can a smart card be used to solve other requirements – can the same 'apple' be used for other applications?

This, in turn, introduces another business concept: value for money. If an enterprise spends a little more, can it achieve a leap in value? This is where the banana becomes so important. The optical memory card (OMC) has been constantly likened to smart cards in an apple-to-apple comparison; however, it's more useful to think of the OMC as a banana.

The banana has been available for some time. It offers additional benefits for a small increment in price; it has wider applicability and is a turnkey solution that comes with risk assessment and security enhancements; and it is supported by a team capable of producing the best practice documentation for deployment and whole-of-life use. You may, however, find yourself in front of the board explaining why the banana is better.

The OMC is being used throughout the world for a variety of applications and solutions. It can hold more technology than any other, is constructed using a polycarbonate with a use-life of 10 years and protects itself through tamper-proof elements embedded during manufacture. It can hold more biometrics than any other card and, at a bare minimum, holds a massive 12 megabits of information. It is the card of choice for India, Canada, USA, Italy, Mexico and other countries, and conforms to ICAO 9303 and ISO/IEC standards, among others.

BEST OF THE BUNCH

So let's look at a hypothetical. I am a defence person being transferred to a political hotspot. In order to check out from my current base I need to go to medical, dental, uniform, mess, stores, pass office, pay office, etc. Can you put all of this information on one card, use the same card to include biometrics and authentication processes and use it as a pass and entry card? If the card is the OMC, the answer is yes, and you can also have a chip, magnetic stripe and barcode on it.

What other options are there for this hypothetical? Use conventional transmission technology that is more expensive and



If an enterprise spends a little more, can it achieve a leap in value?



can cause a massive increase in transmissions when a battalion arrives in the hotspot? Or, alternatively use eight smart cards?

Using this hypothetical, the cardholder need not give up privacy and ownership of the biometrics. The OMC does not need a huge database to match your biometric; the match can occur at the station where you submit your card for matching. You give permission for the use of your biometric when you present that biometric for matching. The system need only send a transaction to a smaller database, stating the match occurred, was valid and it was you using your card.

When we look at this scenario (it's more reality than hypothetical), we see where else such cards could be used to address many requirements at once – possibly as a national ID card that can include electronic visa and passport information. Again, this isn't all that hypothetical (you may want to look at the new Italian ID card as an example).

Upon completion of installation, the true lifecycle of a turnkey solution begins. A capable vendor should seamlessly extract themselves with no impact to the ongoing enterprise processes and application lifecycle. The OMC has been designed as a turnkey, transparent business tool to ensure significant, secure and enduring business requirements. Supported by sound policy and procedural development, where risk is reduced to an acceptable level and where you have a level of comfort that recognises and applies care, prudence and due diligence for those that use it, the OMC is the 'banana' that does it all. Keltec and its associates have formed a partnership based on working relationships with focused, unbiased and non-compromising expertise that brings together a turnkey solution, not just an end product.

So, for those who think you must buy technologies to address only one business need at a time, that don't integrate well with others (such as the smart card) and that don't include policy, process and procedures, then think again. ■