Smart Devices

Technology has a habit of converging – a tendency that can play an important role in anti-counterfeiting, logistics and compliance in the pharmaceutical and medical devices industries

Adrian Burden at Bilcare Technologies

As information technology becomes more sophisticated and electronics become even more powerful on ever smaller scales, technology as a whole tends to converge (1). A good example of this is the smart phone; the combination of a telephone, organiser, music player, camera, road atlas and email device all within one small handheld package.

This kind of merging of technology tends to be consumer-driven and mass-market oriented. But there are plenty of cases where technology is converging in the business world, where the desire to pull several commercial levers with one convenient device is highly appealing. Analogous to the example given above is the commercial personal digital assistant (PDA), which now commonly sees a mobile computer platform integrated with a phone, barcode reader, write-on screen and mapping system. PDAs are often carried by couriers, for example, to enable packages to be delivered to the correct recipient and for the delivery status to be updated in real-time over the internet. The result is improved efficiency, fewer delivery errors and a web-based service for both the sender and the receiver to track progress.

Ultimately, a business looks for devices that will improve the bottom line by driving sales, saving operating costs or improving customer relationships. If several devices can contribute to more than one of these aspects, the opportunity exists to make multiple savings, and technologies are likely to come together.

A Business Case for Anti-Counterfeiting

Most people agree that counterfeit products are a scourge (2,3). In the case of fake pharmaceuticals and medical devices, they represent a real danger to the patient because of the significant harm they can do (4). Businesses also recognise that counterfeits are highly damaging: they reduce sales revenue; they cause warranty problems; they necessitate proactive policing and educational activities and they can cause untold damage to a brand. But equally, many businesses have trouble putting a 'dollar value' to these problems. Measuring the effect of counterfeits on a business is extremely difficult, often because counterfeits are most prevalent in overseas territories where making informative measurements may be hard. It is also problematic to understand if counterfeits represent lost sales or simply additional opportunistic purchases. These subtleties are also different for various markets – fake fashion

accessories do not necessarily have the same health impact as fake pharmaceuticals. However, this is not always the case, as fake sunglasses can have poor ultraviolet protection causing eye damage, and fake cosmetics can cause skin irritation. As a result, consumer behaviour can be markedly different when purchasing different types of products.

Consequently, deploying an anti-counterfeiting solution can seem an expensive investment, requiring a certain amount of cost per unit in terms of a label or a tag that eats away at margins and may make no difference when it is copied or passed-off a few months later.

The Drive for Multiple Benefits

Businesses are often, therefore, trying to 'kill two birds with one stone', or at least 'make two savings with one expense'. This means that if an anti-counterfeiting solution can help address other issues as well, it becomes easier to implement and the user can begin measuring a return on investment without relying so heavily on one outcome.

Solutions that extend automatic identification (Auto-ID) to include authentication (Auto-IDA) are therefore very appealing. Logistics and quality control can then be integrated with the strategy to stem counterfeits and reduce grey market profiteering. Achieving this in a cost-effective manner drives a convergence of technology, as processes and equipment should ideally be capable of reaching both targets without requiring too much additional effort or further devices. We are already starting to see evidence of this convergence in the marketplace. Back-end database systems that enable batches and individual items to be tracked and traced through a supply chain to improve delivery processes and reduce inventory are also being applied to the maintenance of authentication records. In the past, authentication was perhaps managed through a security label like a hologram or covert chemical taggant, but these were often divorced from the logistics process.

Various endeavours to use track and trace as a means for authentication have also surfaced. Certainly it is possible to use a serial number as a means of tightening the supply chain to reduce counterfeiting, but one is always faced with the issue of whether the number presented is the original or a copy. Supporters of this approach claim that once a duplicate arises, the system will provide a timely alert, and with a robust track

and trace system all incidences can be recovered. The issue is that the fake could have been sold or consumed well before it is discovered, or a flood of fakes with legitimate serial numbers could bring such a system to its knees.

Nevertheless, item level serialisation on pharmaceutical and medical devices is likely to become mandatory in a growing number of countries, and information will be collected in the supply chain, on the alleged identity of a product, as well as its authenticity. This will generate an audit trail of pedigree and help squeeze out counterfeits.

Figure 1: A device capable of reading barcodes (above) as well as authenticating a security feature on a packet (right)

As the sophistication and accessibility of the database system increases, the records relating to these processes will extend to additional services, including warranty and after-sales management. The result is comprehensive life cycle management through the integration of IT services that include enterprise resource planning (ERP), customer relationship management (CRM) and returns management (RM). As manufacturers are also being asked to consider their environmental impact through new national and international directives, end-of-life or recycling management is also an area of key concern. In the medical arena for example, there is already a duty of care requirement in many countries to correctly label and dispose of biohazards and medical waste. In the electronics and consumer goods industry, there are also directives for marking and recycling certain components and their associated materials.

This convergence of software-driven processes is relatively easy to understand and probably comes as no surprise, but increasingly there are opportunities to provide multi-purpose devices. An example would be a point-of-sale barcode scanner or credit card payment device equipped with further authentication devices. Datalogic Scanning, for example, announced in March 2010 a barcode scanner unit equipped with ultraviolet light emitting diodes (LEDs) for authenticating banknotes and identification documents (5). This enables one device at the point of sale to process items being sold, authenticate the cash being used, and check the credentials of the purchaser (for example where medicines are being prescribed or alcohol is being sold).

As another example, a sensor for authenticating item-level security technology can be combined with a 2D

barcode scanner, so that a point-of-sale device can process all barcoded items, but when a product that is protected by the specific technology is presented, it can be authenticated using the same equipment, as shown in Figure 1 (6).

Figure 2: Combining DataMatrix labels with embedded security features provides labels that can be tracked, traced and authenticated when combined with a database system

A combination of functions in one device also offers the opportunity to strengthen the level of authentication; rather than it being an offline process, for example by viewing the characteristics of a hologram and undertaking a forensic analysis in a laboratory, this approach enables authentication to take place in real-time at the point of sale, when the medicine is dispensed to a patient. It also ties this authentication record directly with the logistics information, so not only is it clear that the product has been sold and stock is depleted, but the user can also tell that the product was genuine, and any occurrences of counterfeits can be detected and acted upon (see Figure 3).

Convergence of Technology

In the pharmaceutical and medical industry, it is highly likely that we will see even stronger examples of technology convergence where anti-counterfeiting is concerned. There is still a debate about whether a patient should have to be concerned with authenticating medicines and some strongly believe that the last professional in the supply chain (the doctor or pharmacist) should be the one to authenticate. However, with the growth of internet pharmacies – a phenomenon that is not going to abate regardless of the contentious issues that surround it – more and more patients will need to be empowered to authenticate their medication themselves in the comfort of their own home (7).

This approach is particularly relevant to the pharmaceutical industry. Products are beginning to be labelled or marked with 2D barcodes (such as the DataMatrix format; see Figure 2) that might include expiry dates or serial numbers, and at the time of writing the EU Commission is likely to enforce this approach more widely within its member states. The result is that a relatively sophisticated 2D barcode scanner is required to process the product in the pharmacy. However, as products will also increasingly include authentication features, it becomes ideal if the same device is equipped to authenticate. This helps reduce the overall cost of a system, as well as providing multiple benefits to the supply chain, sales process and patient safety.

Although, it is unlikely that members of the public will buy a device in the near to medium term to authenticate medicines if that is its sole purpose. Moreover, the practice of authenticating medicines on a wide scale in the home may actually derive indirectly from another useful function for the patient. We will, therefore, see devices that not only authenticate medicines, but

Figure 3: A screenshot of a database system tracking and tracing items in a supply chain, with authentication information fully integrated within the software

Tag ID	ID	Product	Batch	Manufacture Date	Expiration Date	Authent. Stat.	Service Expiry Date
	urn:epc:id:sgtin:0T6000.0002361.224	AN_MATERIAL1			03.01.2010	Not Authenticated	
	urn:epc:id:sgtin:0T6000.0002361.206	AN_MATERIAL1			06.05.2014	Not Authenticated	
	urn:epc:id:ssoc:000001.88000000001					Not Authenticated	
123	urn:epc:id:gtai:000006.000001.17	RTI_MATERIAL1				Not Authenticated	
	urn:epc:id:sgtin:0T6000.0002361.230	AN_MATERIAL1			01.01.2010	Not Authenticated	
123	urn:epc:id:gtai:000006.000001.8	RTI_MATERIAL1				Not Authenticated	
	urn:epc:id:gai:000001.7		INP1-JUL-2010	20.07.2010	31.12.2013	Not Authenticated	
	urn:epc:id:sgtin:0T6000.0002361.231	AN_MATERIAL1			01.01.2010	Not Authenticated	
						Not Authenticated	
	urn:epc:id:gai:000001.8	IM6	INP1-JUL-2010	20.07.2010	31.12.2013	Not Authenticated	

Figure 4: A handheld industrial PDA with integrated clip-on device for authenticating, amongst other things, pharmaceutical blister packs

also link up to a patient diary system to enhance compliance and make repeat prescriptions easier to process. In addition to this, doctors and patients will have an opportunity to share information appropriately to help understand the effects (and side effects) of a particular course of treatment. This approach is likely to be introduced first for long-term medical treatments or lifestyle medicines. Brand owners will be able to integrate these services with improved logistics to ensure medicines are always in stock. Customer loyalty is also likely to be increased as improved medical compliance and convenience tend to improve the medical outcome, thereby avoiding patients switching unnecessarily to alternative treatments.

The mobile phone is likely to be the anchor for this technology convergence at the consumer level. We are already seeing mobile phone devices combined with heart rate monitors (for example, the Samsung MiCoach system in collaboration with Adidas) or with blood sugar level sensors for diabetes care (from LG Electronics). Nokia also released a phone equipped with a radio frequency identification (RFID) tag reader, and software is now capable of decoding relatively large, low resolution 2D barcodes through images obtained on camera phones. This, then, is the start of consumers being equipped to independently process supply chain information and obtain medical-related/well-being data with their own devices.

Eventually, these same devices will be equipped with other sensors to enable patients to authenticate their medicines, be reminded to take them and record data about their medication and symptoms. There are already examples of industrial PDA devices capable of doing this, as shown in Figure 4.

Conclusion

This convergence of technology will rely on the adoption of global standards by stakeholders. As pharmaceutical manufacturers begin to serialise medicines by marking packaging, so the ubiquitous formats will drive device manufacturers and service providers to innovate. There will also need to be an open approach towards sharing at least some of

the data that this creates. The internet has provided ample evidence of the way processes and services can be enhanced and quickly innovated through a collaborative open-innovation model. As an industry we will need to carefully embrace this thinking if we are to really benefit from technology convergence, reduced operation costs and enhanced services for the customer that could directly or indirectly reduce the problem of counterfeits.

References

1. Schmidt S, *The Coming Convergence: Surprising Ways Diverse Technologies Interact to Shape Our World and Change the Future*, Prometheus Books, 2008
2. Profiting from Fake Pharma, *Bloomberg Businessweek*, 20 August 2007, www.businessweek.com/technology/content/aug2007/tc20070818_443978.htm
3. 'Cancer curing coffee' among thousands of seized drugs, *BBC News*, 14 October 2010, www.bbc.co.uk/news/uk-northern-ireland-11545489
4. For more information on the extent of counterfeits in the pharmaceutical industry as well as other sectors, see www.notofakes.com
5. Datalogic Scanning press release, 8 March 2010, https://easeofaccess.scanning.datalogic.com/public/marketlit/Send.aspx?file=PR20100308-ENA4
6. *Securing Pharma*, 29 July 2010, www.securingpharma.com/40/articles/535.php
7. US to target fake online pill pedlars, *BBC News*, 17 December 2010, www.bbc.co.uk/ news/technology-12017185

About the Author

Adrian Burden is currently responsible for developing the business of Bilcare Technologies in Europe and manages the 'No To Fakes' initiative at www.notofakes.com. He was the co-founding director of Singular ID, an award winning brand protection technology company that spun out from the Institute of Materials Research and Engineering in Singapore. Singular ID was later acquired by Bilcare to create Bilcare Technologies, a company specialising in product, packaging and document security. Adrian has previously worked in the displays industry and provided fee-paid lectures and courses on technology roadmapping for small to medium-sized businesses and organisations. He has an MA from the University of Cambridge and a DPhil from the University of Oxford. He is a Chartered Engineer and a Fellow of the Royal Microscopical Society, where he is currently Scientific Editor for their publication *Infocus*. Email: adrian.burden@bilcare.com