

Taking security systems to the next level

Identity security is a pressing global problem, the prominence of which has led a number of countries to turn to biometric solutions. Their applications are not limited solely to passports, says **Ramji Krishnan** of Datastrip, who explains how his company's work in developing mobile, multi-purpose technology aids both the public and private sector

Over the past three years security officials in the Middle East have witnessed a steady increase in the use of biometric technologies at commercial and government sites. With a number of new biometric applications emerging, ranging from ePassport and National ID verification at airports right through to access card authentication at industrial facilities such as power plants and oil and gas facilities, the Gulf region is alive with opportunity for the manufacturers and suppliers of both ID cards and biometric readers.

Across the world, mobile biometrics solutions are being implemented to verify ID cards, passports and visas for travellers and workers at airports, seaports and border points. The Middle East is among the fastest growing regional economies in the world, thus much is being invested in security at its airports and ports. It's crucial that these kinds of facilities have a security infrastructure in place capable of protecting passengers and the transportation of cargo if growth is to be sustained.

Transportation security – airports and border crossing

While undoubtedly a primary form of identification, the weight attached to passports varies across the world. Although passports are growing in importance internationally, many nations still rely more heavily on visas, travel cards, driver's licenses, national ID cards and health cards for individual identification. As a result, governments need broad point-of-entry solutions capable of performing multiple functions.

Fortunately, point-of-entry technology has evolved significantly over recent years. The emerging mobile, multipurpose technology is now paving the way for nations to accept biometric passports, as well as other travel documents. Advanced ePassport readers can connect wirelessly to back-end systems for biometric identity verification while fewer physical wired connections are required, which thus reduces mobility restrictions and line breakage. Another important feature is extended battery life, which allows guards to carry a unit through a full eight-hour shift without recharging.

security at seaports for workers and cargo requires the convergence of physical and logical security. Complete end-to-end security includes physical and logical data access so as to protect the physical and data assets of ports, while the addition of mobile readers delivers a more complete security solution which allows the authorities to deal with potential threats effectively.

Self-contained, handheld units have been designed to be carried on the guard or border agent, so they go wherever a security guard needs them. This reduces the need to purchase multiple fixed units at each entrance,

Providing effective security at seaports for workers and cargo requires the convergence of physical and logical security. Complete end-to-end security includes physical and logical data access so as to protect the physical and data assets of ports, while the addition of mobile readers delivers a more complete security solution which allows the authorities to deal with potential threats effectively

Of course, we must not overlook the fact that ePassports have not yet been universally adopted. While ePassports are undoubtedly emerging fast and will eventually be the international standard, it's still very important for mobile ePassport readers to be able to comply with relatively dated technologies and scan full pages of old passports – old passports which may not even have a machine readable zone (MRZ). Meanwhile, providing effective

units which require on-the-spot ID verification. Handheld readers also provide access control for manned identity verification at entry points, gates, vehicle sites and other remote access areas.

With global trade and commerce rising year-on-year, maritime security is an area Middle East governments can't ignore. While the need for physical security at ports is well established – over recent times the issue of cargo

security has gained significantly in prominence as well. Indeed, the future of commerce is dependent on the ability of the maritime industry and government agencies to improve cargo security while simultaneously facilitating the efficient flow of goods.

Industrial security

Most corporations have installed some form of physical or logical system for access control at their facilities. Now that biometric technology is affordable and reliable, many corporate security officers are looking to integrate biometrics with their existing security systems. Mobile biometric readers now give facilities the ability to provide identity and access management at more locations than just the front door. Thanks to wireless technology and Internet protocol-based monitoring solutions, corporations can use mobile readers to develop multiple points of manned entry, with each reader transmitting data back to a centralised database for ID verification. This helps ensure that the correct person is in the right place at the right time.

Most of the readers that integrate with existing access control systems provide identity verification for multiple forms of ID. Electronically verifying and logging the IDs of staff and contractors by means of a mobile reader can be done on the spot. This means that the data can be both time and date-stamped and then sent back to the back-end system via wireless network in real time.

Mobile readers are ideally suited to working with applications where accessibility to fixed access locations may not be possible – for example in the event of the emergency evacuation of a facility. Mobile terminals can be used at assembly points to account for those individuals known to

be on-site, either by verifying them against a database residing on the terminal or via a wireless network to the backend server.

Selecting a reader for any sector

Regardless of the application, corporations can maximise their security investments by purchasing mobile biometric readers that meet the following requirements:

- **Rugged, flexible construction.** Mobile readers must be designed to withstand harsh weather conditions and unpredictable movements

- **Field-tested.** Because they perform such a critical function, mobile readers should be field-proven in mission critical environments
- **Long battery life.** Mobile readers that need frequent recharging create downtime, something that is associated with a backlog of traveller traffic and potential gaps in information security
- **Compliance with government specifications.**

Mobile reader manufacturers should be able to verify that their products meet the most up-to-date requirements for biometric equipment, for example the need to be FIPS 201-certified

- **Easy integration with existing ID management systems.** Open platforms that support biometric technologies from multiple providers
- **Simultaneously support multiple applications on the same terminal.** Enhance the utility of the Mobile

terminals is important. Thus they should fulfill various security applications – including reading national ID cards, driver's licenses, physical access control system cards, ePassports – rather than having their usage restricted to a single application

- **Expansion ready.** The ability to connect third-party options via Wi-Fi, GSM/GPRS, USB, CF, serial and Bluetooth® expands memory and enables global communications capabilities, thus increasing the working life of the mobile reader

A final word

Middle Eastern organisations have to overcome some significant hurdles in seeking to integrate mobile technology. The demanding technological requirements of governments and industrial enterprises, the fact that these requirements evolve on a seemingly continual basis in order to keep pace with technological development and the need to work with the existing security infrastructure, all add up to an extremely challenging environment for manufacturers of mobile biometric terminals. With citizens carrying varying forms of identification, officials at government and corporate facilities are tasked with accruing the technological means to accurately read and verify both high-tech and low-tech IDs. Additionally, mobile biometrics must be built to withstand any and all weather conditions so as to ensure there are no security failures in adverse situations.

Investing in mobile biometric technology capable of meeting all of these requirements is the key to good security. In the face of widespread concern about identity security the demands made of biometric terminal manufacturers and solution providers grow ever more stringent, making it crucial that we focus on utilising the latest technologies in the field. Mobile readers are a prime example and, ultimately, they represent the solution for facilities seeking to link ID verification at multiple points of entry to a central access control system. **ES**



Ramji Krishnan is the Vice President - Middle East, Africa and APAC for Datastrip Limited. In this role, he is responsible for the above regional operations from Datastrip's new regional office in Dubai. Krishnan has more than 25 years experience in the field of integrated electronic security and communications systems in India, Singapore and the Middle East.