

Leading the fight against ID document fraud

Passport fraud is a crime with a long history, and the growing sophistication of the counterfeiters is placing great pressure on providers to develop more secure identity verification methods. **Henk-Jan Engelhardt** of Keesing Reference Systems explains how combining biometric technologies with physical security can beat the fraudsters



A traditional safety feature: Kinegram in Dutch ePassport.



Keesing Reference Systems®

Fake documents are a crucial weapon in the fraudsters' armoury. They provide a means for the illegal obtaining of a wide range of goods, services and loans, the effect of which is often felt throughout wider society in terms of organised crime and extremely sophisticated instances of high-level fraud. Passports and ID cards, as one of the primary means of personal identification across the globe, are a particular target for fraudsters, meaning that improving their security is widely recognised as being a goal of crucial importance, something only further underlined by the sheer scale of passport production. "Our estimate is that nowadays approximately 150 million passports are issued worldwide each year," says Henk-Jan Engelhardt, General Manager at Keesing Reference Systems. As a specialist provider of verification tools and solutions that allow international organisations to authenticate ID documents and banknotes, Keesing is at the forefront of the ongoing battle to prevent fraud with ID documents.

This battle is increasingly focused on ePassports, which combine biometric technologies with enhanced physical security features so as to reliably authenticate the citizenship of travellers. "Almost 50 countries will issue a total of 60 to 70 million ePassports in 2008, while in addition almost 30 countries have ePassport programmes under development," notes Engelhardt. "Biometrics are an increasingly important element in the modern passport."

This move towards ePassports, prompted by the enhanced security they offer, is a worldwide trend. However, the global accessibility of the Middle East, allied to its increasing importance as an international business centre and the demographic changes that status brings with it, means that the development of ePassports is being monitored particularly closely in the region. "Several countries in the Middle East are adopting ePassports," explains Engelhardt. "They are motivated by the increasing number of tourists, the exciting economic growth being

experienced by the region as a whole, and the rapid growth in business traffic. The Middle East region is expected to experience average growth in passenger traffic of almost 7 per cent over the next few years, which makes it the fastest growing air travel market in the world. Dubai airport handled over 34 million passengers last year and this is expected to grow to 40 million in 2008. Meanwhile, if we look at Bahrain then we see that over 63 per cent of the country's workforce is comprised of overseas workers. Similarly in Kuwait expatriots make up about 60 per cent of the total population, while Egypt plays host to between 1.5 and 3 million Sudanese citizens."

While this kind of large-scale migration has undoubtedly brought real economic benefits to the Middle East, it has also brought with it significant pressures in terms of documentation and security. These are pressures to which the authorities across the region have responded. "It has been estimated Egypt will issue between 500,000 and 700,000 ePassports in 2008," says

Engelhardt, pointing to one of the more prominent countries in the region to adopt ePassports, a development which has encouraged a number of other nations to follow suit. "The United Arab Emirates will roll out 5 million eID cards over the coming three to four years," continues Engelhardt. "It is expected that Turkey will issue between 1.5 and 3 million ePassports in 2008 and that Qatar will issue at least 4 million over the same time period."

Technical challenges

Although it is clear that the adoption of ePassports amongst Middle Eastern nations will reach critical mass soon, a number of significant technical challenges remain in terms of their overall implementation. Prime amongst them are the three main areas defined by the International Civil Aviation Organisation (ICAO) as being particularly crucial to the development of ePassports – security, interoperability and facilitation. "Basic Access Control and passive authentication have now been made mandatory by the ICAO, while they also recommend Extended Access Control (EAC)," says Engelhardt. "EAC standards are still in the development phase, thus operational interoperability and

facilitation are at a similar stage. As a consequence, the number of readers capable of reading ePassports at border crossings is still limited. So, although roughly half of the passports issued today are ePassports, the other half are still non-ePassports. Meanwhile, even in those countries that do issue ePassports many traditional passports remain in circulation, a situation likely to persist for up to 10 years."

Clearly much work remains to be done, not least in terms of the underlying ePassport infrastructure. While the passports themselves are increasingly standardised, the same cannot yet be said of the readers, something which has real implications at a practical level. "Readers, and the often complex systems which underpin them, remain relatively costly," says Engelhardt. "Such systems are especially crucial in border situations. However, borders are not the only places where fraudsters can be caught. In fact, these people know there will be extensive inspections when crossing borders so they'll often try to avoid these inspections. In general passport readers and the systems which

underpin them are too expensive for hotels, car rental companies, HR managers and even banks, despite the high losses they suffer as a consequence of ID document fraud and illegal labour."

While biometric technologies undoubtedly represent an important step forward in document security, these kinds of practical concerns demonstrate that traditional security features should not be abandoned. Indeed, Engelhardt is keen to stress that they still have an important role to play, an approach which serves to further emphasise the overall maturity of biometric solutions. "There are many situations in which the chip cannot be read, in which the equipment required to read the chip is missing, or in which the passport does not even contain a chip," he acknowledges. "This is one reason why we should always verify physical security features, such as watermark and UV. We often call these traditional security features, but they have undergone rapid technological development themselves. Even if all passports were ePassports, and even if all readers were able to read the chips in them and be available anywhere, traditional security features would still be extremely important."





Keesing Passport Reader

Keesing Reference Systems®

Regional challenges

In addition to the common problems experienced by countries that have surfaced when attempting to adapt technology to reading passports there are technical challenges that are unique to the Middle East regions. Henk-Jan Engelhardt sites a project to illustrate this point; “A very interesting project related to the Middle East currently running is the Arabic transliteration project. By request of ICAO a taskforce

in many ways into Latin; Mahmut, Mahmud, Mahmood, Mehmood, etc. Combinations of first names and sir names even have many more variations.”

The need to keep pace

With ePassport programmes having been successfully implemented across the Middle East, and the number of visitors to the region growing, the need for accurate, reliable, verification of ID documents is acute.


.....

With ePassport programmes having been successfully implemented across the Middle East, and the number of visitors to the region growing, the need for accurate, reliable, verification of ID documents is acute

.....

of ISO/IEC called JTC1/SC17 WG3/TF3 (WG3/TF3 in short) is studying for a solution to translate Arabic characters to Latin characters.

“The eye readable part of passports can be written in several languages with different characters, such as standard Arabic, Farsi, Urdu and Pashto, but the machine readable part (which is read by the readers) can only be written in Latin characters because readers are not able to read non Latin characters. The task force is defining a transliteration table which translates Arabic characters 1-on-1 into Latin characters. A great challenge is the fact that the Arabic writing of the first name Mahmoud could be translated

Airport infrastructure is developing in line with these emerging demands – new immigration control gates are scheduled to open this year at Cairo Airport as part of one of the most ambitious airport projects ever built in the Middle East – the new Cairo International Airport Terminal 3, and verification technology must keep pace. This is an ongoing battle, something that Keesing, having been established in 1923, is particularly well-placed to understand. The lessons of the past are of enormous relevance to the challenges of the future, through embracing its own history the company is maintaining and building on its position at the forefront of ID security development. 



Henk-Jan Engelhardt has worked as General Manager at Keesing Reference Systems for several years now. Prior to assuming his current role he worked for the company as interim manager of marketing & sales, while he also has experience in management positions at a number of traditional media and new media companies.
www.keesingfightfraud.com