Next Generation Border Crossing: ePassports and Their Impact on Border Control

Björn Brecht
Bundesdruckerei GmbH

Over the course of recent decades, new security features and more complex production methods have made passports safer and better protected against forgery and manipulation. Although the quality and level of passport security today still differ from country to country, each new generation of passports has brought with it significant improvements. The EU requirements for the introduction of electronic passports, however, have triggered a revolutionary leap in technology. The integration of an electronic storage medium and crypto-processor into the traditional document in order to store biometric features in the passport and to be able to read this as required cannot be compared with any of the earlier, gradual improvements.

The introduction of ePassports in the EU member states and other countries – an expected total of 70 countries by 2010 – is not a means in itself. In future, the documents will serve as a basis for more extensive security checks at borders and hence as an important part of efforts to curb border-crossing terrorism, organised crime and also illegal migration. A key question is how border crossing processes can be accelerated even as complexity and security requirements increase. Since acceptance and market penetration of electronic passports are increasing, there appears to be a valid argument for using these passports for traveller facilitation at border checkpoints. Whilst a traveller's identity is now checked at the border merely by comparing the photo in the passport with the face of the person presenting the passport, this could be carried out in future by verifying the live biometric data captured with the reference data stored on the chip. In an official communication in July 2006, the EU

Commission emphasised the importance of biometric technologies for future border control.[1]

At the same time international traveller numbers keep rising. Growing wealth and globalized business are giving more and more people the opportunity to travel. The number of air passengers alone rose by 5.9% in 2006.[2] Statistics show that this number will continue to increase at about 5% per year, meaning that it will more than double within the next 20 years.[3] Although a large portion of international travellers are air passengers, travellers entering a country via land and sea borders should also be considered. Moreover, illegal migration continues to be a serious border management problem of developed countries.

In combination, these issues will put an enormous strain on border control infrastructures and require more technological and human resources in order to be solved. Processes at borders will change, and new technologies could be enablers for intelligent process redesign.

As traveller numbers increase, so too does the variety of ID documents. With the growing market penetration of ePassports, border guards will have to check non-electronic passports and electronic passports with a single biometric identifier as well as those with two or more identifiers. These passport variations can occur in combination with different kinds of visas, including those without biometrics, biometrics in databases or even biometrics on an integrated chip. Border guards always have to know how a certain traveller and their documents need to be controlled according to national and international regulations.

In addition to ID document variations, border guards will increasingly have to use information systems. One of the large-scale IT systems currently being developed in the European Union is the Schengen Information System II (SIS

[1] Commission of the European Communities (2006), p. 5.

[2] IATA (2007).

[3] Deutsche Bank Research (2006), p. 4.

II). Although discussions regarding storage of biometric identifiers in the system are still underway, SIS II will certainly have a high impact on border control processes. Moreover, in an attempt to boost visa and visa issuing security and to minimise the potential for visa fraud, the EU will store biographic and biometric data of visa applicants in the Visa Information System (VIS). The development of the Visa Information System is leading to the joint updating and use of biometric data stocks by consular offices, border police, security authorities and other users. VIS will then be used by border control authorities to check the traveller's visa data.

As a consequence, border control processes will be extensively integrated with visa application procedures, and part of control work will be moved upstream. This especially means that all risk profiling activities can be conducted as soon as a visa applicant has been enrolled at the consular posts – this has not been possible up to now. Visa issuing officers can then base their decisions on the results of risk profiling and deny visa issuance, or the border guard can deny entry at the port of entry. Risk profiling and joint decisions by consular and border authorities will require new cooperation models and procedures.

Major change will evolve from the growing degree of automation in border control. In recent years, several Registered Traveller Programmes have proven the potential of biometrics for automated border control but most of the programmes were not integrated to regular border control and did not make use of the advantage of biometrics stored in electronic passports. In future, there will be various options for automating the border control process. One option could be an interoperable European Registered Traveller Programme based on the verification of biometric identifiers. In this context, the European Commission’s Directorate-General Justice, Security and Freedom conducted a study to assess perspectives of a European Registered Traveller Programme. In the long-term, automated border control – however, supervised by border guards focusing on high risk travellers – could even be extended to the majority of low-risk travellers using electronic passports.

In any case, the control procedure will change dramatically. Border guards’ work will become more complex and require more sophisticated supporting tools.

Whilst staff today usually conduct visual inspections of passports and additional documents, or simply send data queries to the systems of the security authorities in the native country, they will in future be faced with having to use complex hardware and software. They will have to consider a diversity of process steps, depending on the individual background of the traveller and their travel document.

Full page readers that are able to check not only the MRZ but also perform automated forgery detection will become standard. Automated forgery detection uses pattern recognition methods to match the image of the traveller's document with reference images stored in a database. Moreover, travel document readers will have to be able to read eMRTD chips. Such document reading devices should be part of integrated border control solutions that are also able to handle the entire workflow and reduce complexity for border guards. For example, border posts must also be equipped with biometric sensors such as cameras or fingerprint readers and software that handle biometric and other data along with managing and documenting the control workflow. They must also feature interfaces with national and international information systems.

Additional challenges arise due to the European Union's requirement to store fingerprints on Member States' electronic passports starting in summer 2009 latest. Extended Access Control has been specified as the mandatory security mechanism to protect access to sensitive fingerprints data on passport chips.[4] How does Extended Access Control influence future border control? In order to read EAC-protected fingerprints from electronic passports and conduct live verifications, border posts must be connected to a Public Key Infrastructure (PKI) and this will require significant organizational, infrastructural and technological effort for countries.

[4] Extended Access Control (EAC) is a combination of security mechanisms based on mutual authentication of chip and reading device (terminal). Only authorized terminals can access data protected with EAC. Authorization can only be issued by superordinated certification authorities. Key management requires connection to a Public Key Infrastructure.

Finally, such a border control solution must be able to evaluate captured data as well as answers to search queries, and give border guards recommendations to support their decisions. Integrated border control solutions are still not very widespread but will become more common in future, freeing border guards from more simple control tasks so that their valuable human resources can be assigned to the few high-risk travellers.

As a consequence of these developments, processes at borders will have to be reorganized. The complexity and variation of border control procedures will require new concepts on how to support border guards in their work and integrate border control into a constant horizontal travel chain. Regardless of the efforts that are necessary to implement next generation border crossing procedures, these developments will provide the unique opportunity to boost our national security and enhance traveller convenience.

References

Commission of the European Communities (2006):
Communication from the Commission on Policy priorities in the fight against illegal immigration of third-country nationals, Brussels, 19.7.2006, COM(2006) 402 final.

Deutsche Bank Research (2006):
Zukunft der Drehkreuzstrategie im Luftverkehr, in: Deutsche Bank Research (eds) (2006), Aktuelle Themen 354, 30.05.2006.

IATA (2007):
http://www.iata.org/pressroom/pr/2007-01-29-02.htm