FAL/12-IP/2
3/12/03
Revised
19/1/04
English and French only[1]

FACILITATION (FAL) DIVISION — TWELFTH SESSION

Cairo, Egypt, 22 March to 2 April 2004

Agenda Item 2: Facilitation and security of travel documents and border control formalities
2.2: Biometrics

BIOMETRICS

(Presented by the European Civil Aviation Conference (ECAC)[2])

SUMMARY

This information paper presents to the Division an overview of the most relevant initiatives and experiences of several Member States of the European Civil Aviation Conference with biometrics since the last session of the Division. This information may be helpful to the Division in looking for a worldwide approach for application of biometrics.

1. During the opening of the eleventh session of the Facilitation Division in April 1995, reference was already made to the initial developments in the field of biometrics and the full automation of clearance procedures. The purpose of this Information Paper is to inform the participants of the twelfth session of the Facilitation Division, based on practical information, about the initiatives and experiences that have been acquired with the application of biometrics by several Member States of ECAC in the field of issue and inspection of travel documents during border control and to inform the participants of what developments are taking place in this area within the European Union. This information may be helpful to the participants during the twelfth session of the Facilitation Division in looking for a worldwide approach for the application of biometrics.

2. The Attachment covers the initiatives and experiences of certain ECAC Member States: Germany, Iceland, the Netherlands, Spain and the United Kingdom.

3. The airline industry and authorities have in recent years been faced with an increasingly greater challenge to guarantee the security of international civil aviation. Moreover it is not only

[1] French version provided by the European Civil Aviation Conference.

[2] Albania, Armenia, **Austria**, Azerbaijan, **Belgium**, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, **Denmark**, Estonia, **Finland**, **France**, **Germany**, **Greece**, Hungary, Iceland, **Ireland, Italy**, Latvia, Lithuania, **Luxembourg**, Malta, Moldova, Monaco, **Netherlands**, Norway, Poland, **Portugal**, Romania, Serbia and Montenegro, Slovakia, Slovenia, **Spain, Sweden**, Switzerland, The former Yugoslav Republic of Macedonia, Turkey, Ukraine, **United Kingdom** (the 15 Member States of the European Union (EU) appear in bold).

important that the airline industry itself may be the target, but also that people from terrorist organizations may travel across the world by air, whether or not using the facilities of existing illegal immigration networks and *modi operandi.*

4. In addition to the increased security risks the increase in illegal immigration has caused additional problems for the airline industry and authorities in recent years.

5. The increased security risks and the need to combat illegal immigration effectively have put pressure on the facilitation of international civil aviation. This has increasingly resulted in congestion problems at airports, delays to aircraft, passengers, crew and cargo.

6. In the interests of facilitating civil aviation it is therefore very important that the airline industry and authorities develop new strategies and technologies that, on the one hand, effect the optimum protection of international civil aviation, hamper the freedom of movement of terrorist organizations by air and prevent illegal immigration by air as effectively as possible, and, on the other hand, at the same time facilitate civil aviation to the optimum.

7. The increased security risks and the need to effectively combat illegal immigration in particular require measures aimed at hampering the use of a false identity and discovering the true identity of passengers.

8. Partly against the background of a worldwide growth in passenger volume, the use of biometric elements in the recognition and verification of people when searching for the right balance between facilitation and safety forms a very important key. In particular the following applications of biometrics potentially offer possibilities for looking for new strategies for the facilitation of international civil aviation:

a) the security of the issue of travel and identity documents (including visa) by using biometric data may prevent fraud with these documents more effectively;

b) the inclusion of biometric data in travel documents (including visa), preferably in the machine readable zone, offers possibilities for a quick and reliable automatic inspection of travel documents (including visa) during border control;

c) the inclusion of biometric data in travel documents (including visa) makes it possible in the long term with respect to Advanced Passenger Information (API) that before the arrival of the flight the identity of passengers can already be quickly and reliably verified and clearance procedures accelerated; and

d) the use of biometric recognition systems can contribute to increasing airport security. In particular one can think here of the security access as well as surveillance in the direct transit areas.

9. For a worldwide approach for using biometrics in the facilitation of civil aviation, the following aspects, among others, are important:

a) the choice of authorities of a biometric datum is prompted by different factors for each country. It is not only safety and reliability that are important, but also aspects such as customer-friendliness, the state of the art and investment costs are decisive in the choice of the type of biometric datum. Furthermore, authorities not only have an interest in harmonising the use of biometric applications for clearance of goods, persons and security controls with regard to civil aviation, but also with other national policy areas, such as the surveillance of aliens staying in the national

territory. In addition within these other policy fields use is already made of a certain biometric application and compatibility with these applications is preferable;

b) the choice of a biometric application depends on the purpose for which it will be used and the specific physical environment within which the application takes place. For example a passive form of surveillance of passengers remaining in airport terminals (gates and direct transit areas) in principle requires a different biometric set-up than the automatic inspection during a border control;

c) for a worldwide application of biometrics within civil aviation the compatibility of the stored biometric data is also important. The authorities of various countries, in particular the Contracting States of ICAO, must be able to read one another's biometric data. Important here among other things is the way in which the biometric data are stored, for example the use of a template or digital storage;

d) when developing a worldwide approach for the application of biometrics one must take into account the many actors and control procedures. Not only are several authorities entrusted in each country with different types of controls (border, security and goods control), but also in some cases private companies like airlines have a responsibility in the field of control of travel documents and security;

e) finally, aspects of privacy have a great influence on the possible applications of biometrics. Aspects that are related to this include the exchange of data with authorities from other countries, with private companies, for what purpose the data may be used and how long data may be stored. These questions depend very much on the national legislation and regulations and are hence answered differently by each country.

10. CONCLUSION

10.1 Since the eleventh session of the Facilitation Division in 1995, several Member States of ECAC have gained experience with the application of biometrics. This information paper covers initiatives and experiences of ECAC Member States: Germany, Iceland, the Netherlands, Spain and the United Kingdom. For the participants of the twelfth session of the Facilitation Division this general information may be helpful in looking for a worldwide approach, but it may also be helpful for countries that are considering the implementation of biometric applications.

— — — — — — — —

ATTACHMENT

This Attachment contains the initiatives and experiences of ECAC Member States with biometrics. These are:

GERMANY

– Automatic biometrics-supported Border Control (ABG)

ICELAND

– Facial Recognition System (FACIT)

THE NETHERLANDS

– Automated Border Passage (AGP)
– Visa pilot-project

SPAIN

– "Facelt" based on facial recognition

UNITED KINGDOM

– Automated Border Entry System (IRIS)
– Immigration and Asylum Fingerprint System (IAFS)

— — — — — — — —

GERMANY

Automatic biometrics-supported Border Control (ABG)

Field of application
Passport Control.

Biometric element and reasons for choice
Iris.

Method of storing biometric data
Template with data base linked to a LAN (for the storage of data) with a link to the national Police and EU-SCHENGEN information system (for the retrieval in crime records).

Target group
Bona-fide-persons at least 18 years old; EU/EEA-Member States (Belgium, Denmark, Germany, France, Finland, Greece, Iceland, Italy, Luxembourg, the Netherlands, Austria, Portugal, Sweden, Spain) or citizenship of Switzerland.

Purpose
Germany is planning to use biometric procedures in a number of different areas to improve the security of its citizens. The aim is to make use of specific physiological features to:

a) clearly assign personal documents to their holder by matching a person's biometric feature with the feature stored on the document; and

b) grant people certain rights (such as access to security-sensitive areas) by matching their biometric features with those stored in a previously defined user pool.

Biometric features should be introduced as soon as possible, but in view of considerable investments required not hastily. A national solo-run should be avoided. Only solutions, which are developed in a coordinated approach at international level and which are interoperable, will promise success for the use of biometric systems and will thus improve security. For this reason, Germany seeks close cooperation at international level.

Germany pursues a graded strategy for the introduction of biometric procedures, which is partially reversible. In a first step, Germany's focus is on documents issued to foreigners. Given their long validity and the large number of documents, the introduction of biometric features in passports and identity cards will be postponed for the moment. A sustainable decision on which biometric procedure should be used for these documents will be taken on the basis of comprehensive practical tests. These tests are currently being implemented so that concrete results of the practical use of biometric procedures are not yet available.

In the long term, a contactless chip will be integrated into documents for foreigners and into German travel documents. In a joint initiative, France and Germany have been advocating an amendment to the relevant EU directives which do not yet permit the integration of such a chip.

Description of the system
The ABG-system is designed to operate fully automatically as a passport control system. First the enrolment process is executed in the so-called enrolment-centre. Here a template of the person's iris is generated and a back check is done by the border control authorities. Then an auto-control procedure will

be implemented by identifying and verifying the authenticity and lawfulness of an enrolled person in any case of border crossing. Border police officers will only intervene in cases of irregularity.

Reliability of the system
As the planned pilot project at Frankfurt/Main International Airport had to be postponed for legal reasons for the time being there is no expertise gained in terms of reliability.

Conclusions and present situation
Actually there are no outcomes; kick-off for the pilot (time frame six-month) will presumably be end of the year 2003.

— — — — — — — —

ICELAND

Facial Recognition System (FACIT)

Field of application
Surveillance system in the airport terminal.

Biometric element and reasons for choice
Facial recognition system.

Method of storing biometric data
In the computer.

Target group
Terrorists, wanted people, individuals who are for some reason not allowed to enter or leave the country.

Purpose
The purpose is to increase the security and possibility to apprehend and stop individuals who are a danger to flight security and other security.

Description of the system
FACIT system works in the way that it measures the distance between certain points of the upper face of the passenger, especially the dark spots of the eyes, and compares them to individuals in the database in order to find a match.

The FACIT system is connected to the terminal surveillance system that consists of 80 cameras whereof three can be connected to the FACIT system each time. The cameras connected to the system are located at certain points that every passenger entering the terminal passes through. The system collects pictures of these passengers and compares them to a database of individuals that are wanted or considered dangerous.

Reliability of the system
The system is under constant development. It catches up to 99 per cent of the faces of passengers though the matching percentage is considerably lower. The lower matching percentage is mostly due to low quality photos of wanted individuals in the database. The final analysis of whether the match is reliable is always up to the officer working with the system.

Conclusions and present situation
FACIT has proven to be a helpful tool in case of investigations of individuals passing through. In the future it is expected to improve even more with upgrade of the software which will lead to better quality of the photos in the database.

— — — — — — — —

THE NETHERLANDS

1. Automatic Border Passage (AGP)

Field of application
Passport control.

Biometric element and reasons for choice
Iris.

The iris has been chosen because it shows a high accuracy in recognition and is easy to use. One iris is sufficient and no complicated procedure on the part of the client or passenger is required. Furthermore, the iris of each person is unique and stable over the years.

Method of storing biometric data
Template.

Target group
AGP is accessible to all subjects of the Member States of the European Union, of the Member States of the European Economic Area and to all subjects of Switzerland.

The restriction to this target group is tied up with the fact that other nationalities also have to be checked during the border control for the purpose and the duration of their proposed stay in the Netherlands. This in principle requires handing over documents and an interview with the passenger by the border control authorities and cannot therefore be automated.

Purpose
The purpose of AGP is to automate and speed up passport control (verification of persons) in a simple and reliable way.

Description of the system
AGP makes fully automatic passport control possible, without the intervention of the border control authorities. AGP is an initiative of the airport operator of Amsterdam Schiphol Airport and in cooperation with the government was introduced in October 2001. After a trial period of one year AGP was taken into permanent use with effect from October 2002. AGP is the property of the airport operator.

People can pay to use the AGP service. To be eligible for AGP, the iris data of the person are stored in a template on a personal (smart) card. This personal card is only issued when the border control authorities have established the identity of the person and have checked the validity and authenticity of the travel document and the person is not listed in the police files. The AGP card can never be valid for longer than the validity of the travel document.

A total of 8 AGP gates have been installed at every permanent passport control point at Amsterdam Schiphol Airport, both in arrivals, transit and departures. To complete the automatic passport control three decision points are required.

1) Firstly, the person who wants to use AGP must present their AGP card to the card reader. By doing this, the person also indicates that they want to cross the border. The computer reads the template and checks the validity of the card. If this is in order, the first revolving door is opened and the person is given access to the iris recognition system.

2) The person must present their eye for the iris scan. The police files are then consulted in a secure way to check whether the person is listed. This is the second control point.

3) These data-files are of course not accessible to the airport operator and are made secure by fire walls.

4) Finally, the iris recognition system assesses whether the iris presented corresponds with the iris data of the previously presented AGP card. This is the verification and the third decision point. If the iris can be verified and the person is also not listed in the police files, the second door automatically opens. The person can leave the AGP gate and the automatic passport control is completed. The verification of the iris takes between 3 and 7 seconds.

If the iris presented by the person does not correspond with iris data on the personal card or if the person is listed in the police files, the person is automatically directed via a revolving door to the normal passport control. The border control officer is at the same time given a silent, visual alarm that the person in question was not accepted by the AGP system. The AGP systems are located such that the border control authorities have a direct view of them. The border control authorities can also overrule the system manually at any time.

Reliability of the system
The reliability as regards the false reject rate (FRR) is affected in general by the physical environment such as the light conditions, but also how the person presents their iris to the iris recognition system. With regard to the false accept rate (FAR), there is less than a 1 in 70,000 chance of the AGP system accepting the iris of a person based on someone else's iris data. The reliability is even greater if one also has to take into account the fact that the impostor also has to have thousands of stolen AGP cards to have one with a comparable iris. This means that the system performs better than the human being. The system is also protected against abuse and for example takes into account the three dimensional structure of the eye. This data is confidential.

Conclusions and present situation
AGP has been structurally implemented at Amsterdam Schiphol Airport and has a still growing number of participants. Based on extensive testing by independent research bureau the AGP system has been assessed as extremely reliable. Furthermore the system is being regularly assessed over time.

2. **Visa pilot-project**

Field of application
Entry control persons (Visa and passport control).

Biometric element and reasons for choice
Fingerprints and facial recognition.

Two different biometric elements were chosen in order to be able to compare their reliability and accuracy under “real” circumstances.

Method of storing biometric data
Template/image (CD-ROM).

Target group
Subjects of States that need visa to enter the Netherlands or to transfer via the Netherlands were the target group. The system was tested on passengers travelling from Accra, Ghana, to Amsterdam Schiphol airport.
As the two different systems (fingerprints and facial recognition) were tested in the context of a pilot-project the participation was voluntary. The pilot-project foresaw the participation of 300 persons. About 65 per cent of the people that formed part of the target group agreed to participate. As a consequence the pilot-project could be run in little under one month

Purpose
The purpose of introducing the capture of biometric features into the visa issuance procedure is to combat the phenomena of illegal immigration. By way of creating a link (biometric feature) between the individual and the visa issued, once the individual arrives at Amsterdam Schiphol airport, it can be determined whether the person travelling with a certain travel document in which a visa is included, is the individual to whom the visa was issued.

Also in case an undocumented person arrived on the flight from Accra, Ghana, it can be verified against the database of people that was issued a visa by the Netherlands diplomatic representation in Accra.

Description of the system
The pilot-project was run on the Netherlands diplomatic representation in Accra, Ghana, and on Amsterdam Schiphol airport. Once a visa application of an alien that wanted to travel to or via the Netherlands was approved, the alien was asked to participate voluntarily in the pilot-project. Participation implied the capture of two fingerprints (finger of both right and left hand), the making of a photo of the face and the scanning of the passport. Both biometric features were stored on a CD-ROM that was flown the next day to Amsterdam Schiphol airport. There the CD-ROM was read out and the information was stored in a local database. Once the participating alien arrived at Amsterdam Schiphol airport his or her fingerprint and photo were taken at the gate of arrival and the passport was scanned (verification). The system would indicate separately whether there was a match on the fingerprint and the face (one to one comparison). In case the verification failed or an alien without any travel document arrived the system could be switched to the identification mode (one to many comparison).

Reliability of the system
As far as the fingerprint part of the pilot-project was concerned 100 per cent reliability (accuracy) was achieved both for verification and identification purposes. The face recognition feature was not able to recognise the alien in 18 per cent of the cases in the verification mode. When used for identification purposes it failed to recognise the person in 22 per cent of the cases. Medio ambiental circumstances (light conditions) as well as specific features of the face of the persons captured seem to influence strongly the reliability (accuracy) of the facial recognition system.

Conclusions and present situation
The pilot-project as it was held between Accra and Amsterdam proved to be a success. The practical usefulness of systems that use biometrics was underlined. This was certainly true for the fingerprint system. The facial recognition system will need some additional attention to take away the distorting elements that are of influence on the results obtained with that system. This might lead to a better matching rate than the one achieved so far.

It is foreseen that another pilot-project with the same two systems will be held between Beijing, China and Amsterdam Schiphol airport during the autumn of 2003.

— — — — — — — —

SPAIN

"FaceIt" based on facial recognition

Field of application
Control of persons.

Biometric element and reason for choice
Facial recognition will be used. This system, apart from being very precise, will allow for a real-time identification of persons.

Method of storing biometric data
Image.

Target group
All persons, independent of their nationality. It can be used in whatever location.

Purpose
All persons. It can be used for the identification and localization of wanted persons or persons that have disappeared; for facilitation and speeding up border control and for the fight against falsification of documents.

Description of the system
This system is installed, as an experiment, in the airport of Madrid-Barajas. The functioning of this application consists of a camera, appropriately installed, that captures automatically an image of the person that is waiting in line for passport control. One of the advantages of the system is that the persons that are the object of the control do not know that a photo is being taken of them. As a consequence there is not need for any collaboration on the part of the individual.

Once the image is captured, it is processed by the system and a certain geometric pattern is extracted. This pattern is obtained by taking measurements that convert every face into a digital code. Once the pattern, identified by a digital code, is obtained, the system gives, by way of the creation of templates, the possible images that may coincide with the images that were previously stored in a database so that people can be identified. The time needed for the processing, comparison and answer is between four and five seconds.

This system can be combined with the so-called Border Guard-Face watch that, by way of a photographic process of the biographic page of the travel document, apart from analysing the authenticity of the document and detecting of possible falsifications, makes a comparison between the geometric features of the face of the person that presents him-/herself to the border control and the geometric features of the photo included in the travel document.

Reliability of the system
In general terms the reliability of the system is affected by medio ambiental circumstances, especially by the light intensity at the moment of the capture of the image. The system potentially gives a very high percentage of matches, more than 90 per cent.

Conclusions and present situation
This system is actually installed and going through a test phase at the airport of Madrid-Barajas. In view of the results that were obtained so far by using the system the border control officers consider it to be an useful system that facilitates the control and contributes to a more efficient detection of falsifications of documents and of impersonations.

— — — — — — — —

UNITED KINGDOM

1. Automated Border Entry System (IRIS)

Field of application
Certain enrolled passengers (categories yet to be finalized) will be able to gain entry to the UK via an automated border entry system. The project is currently at the procurement stage.

Biometric element and reasons for choice
Iris.

Iris recognition has been chosen because it will provide a fast, fraud-resistant way to pass through UK immigration controls.

Method of storing biometric data
Probably iris code and image.

Target group
The precise target groups have yet to be finalised but the system is aimed at expediting clearance of low-risk frequent travellers at selected ports in the UK.

Purpose
The proposal for IRIS is based on the use of iris recognition technology to enable automated border entry. The implementation of IRIS will remove the need for pre-enrolled passengers in certain categories to be seen in person by the immigration officer on arrival in the UK. The system will:

- speed up the admission of genuine travellers;
- reduce the possibility of identity fraud and; and
- enable immigration officers to concentrate on higher priorities.

A trial using iris recognition technology was conducted at Heathrow Airport between January and July 2002 in conjunction with the Simplifying Passenger Travel (SPT) Group. The objective of the trial was to prove the concept of expediting the arrival process at immigration for participating passengers, as well as proving the use of iris recognition as an enabling technology.

The SPT UK Regional Group's report of the trial concluded that it had been successful in meeting a range of objectives in that (in summary):

- it simplified and expedited the arrivals process at immigration for participating passengers;
- it demonstrated that iris recognition is a safe, effective and robust technology in a live airport environment;
- it showed that the technology can positively identify enrolled individuals without the need for either supporting documents or a smart card;
- positive feedback was obtained from passengers - comments from participants were highly favourable;
- it proved that a number of airport-related organisations with diverse functions could work successfully to introduce passengers to an innovative technology;
- it showed that enrolment can be achieved remotely (at JFK in New York and Washington Dulles airport for the purposes of the trial); and
- border integrity was maintained through strict selection criteria for trial participants and verification of identity by an immigration officer on first arrival.

The UK now plans to implement IRIS at selected airports in the UK as a means of expediting passenger clearance and improving the effectiveness and deployment of immigration control resources.

Description of the system
Biometric registration – legislative background

- Primary legislation supporting biometric registration of travellers to the UK is contained in the Nationality, Immigration and Asylum Act 2002. Under section 126 of the Act ("the compulsory provision"), the Secretary of State may require an application for leave to enter or remain in the UK to be accompanied by registration of a person's external physical characteristics. Section 127 of the Act ("the voluntary provision") provides for the operation of a voluntary scheme in connection with entry to the UK.

- In accordance with the voluntary provision, the UK has recently commenced the procurement stage of a project that will culminate in the operation of a scheme whereby registered individuals will benefit from expedited clearance on arrival in the UK, using iris recognition automated barriers.

- The UK is giving further consideration to the implementation of the compulsory provision. This provision will require secondary legislation before it is implemented.

Biometric registration – IRIS RECOGNITION IMMIGRATION SYSTEM (IRIS)

- The UK's Immigration and Nationality Directorate has commenced a project to implement an automated border entry system using iris recognition technology.

- Certain enrolled passengers (categories yet to be finalised) will be able to gain entry to the UK via an automated border entry system that can recognise their iris pattern.

- IRIS will provide a fast, fraud-resistant way to pass through UK immigration controls and allow immigration control staff to concentrate on other priorities. It is envisaged that IRIS will be operational in 2004.

- The IRIS project is now in the procurement stage of implementation. A notice inviting expressions of interest from potential suppliers of technology was published in the Official Journal of the European Communities (OJEC) in early June, with a deadline of 15 July for responses. Those responses are currently under consideration.

Reliability of the system
Not yet applicable for the full operational system. Results of the trial outlined above.

Conclusions and present situation
Not yet applicable for the full operational system.

2. Immigration and Asylum Fingerprint System (IAFS)

Field of application
Immigration applicant identification, mostly used for asylum seekers.

Biometric element and reasons for choice
Fingerprints.

Fingerprints were used for the following reasons: mature technology, high accuracy, large number of legacy fingerprint records, compatibility with police biometric systems, commitment to connect with Eurodac. More recently a trial checking asylum prints against Visa Applicants is underway.

Method of storing biometric data
Ten print image sets (rolled and plains) and templates are stored in the database. Templates of two index fingers are stored in micro chips on Application Registration (identity) cards produced by the system.

Target group
Fingerprints are taken from several categories of applicants including asylum seekers, those who have inadequate travel documents, a section of those refused permission to enter the UK and certain other immigration offender types plus dependants of any category. In practice well over 90 per cent of those fingerprinted are asylum applicants.

Purpose
The purpose of IAFS is to enable positive identification of those enrolled and reduce fraud in the asylum process by preventing the creation of multiple identities.

Description of the system
IAFS (Immigration and Asylum Fingerprint System)

IAFS is based on a fairly conventional AFIS system. The central system is housed in our Headquarters in Croydon, South London and is administered by a System Management Team. Also at Croydon is the Immigration Fingerprint Bureau (IFB) responsible for carrying out expert verification work of potential hits.

The Asylum Screening Unit (ASU, also at Croydon) processes most of those applicants who wish to claim asylum subsequent to entry into the UK, about 40 per cent of the total. They are equipped with five LiveScan units to allow for fast, efficient and inkless processing. At major ports and offices there are around 25 "CardScan" workstations. These allow traditionally inked fingerprint forms to be scanned and transmitted to the central system.

Fingerprint records from LiveScans and CardScans are processed similarly: there is an automated search against existing records and a provisional result is transmitted to the originating unit within minutes, where required files are referred for manual intervention by experts for verification and/or quality control work. Enrolment must take place through either a LiveScan or CardScan terminal. Overall the system has reduced the multiple application rate from c.6 per cent to c.1 per cent.

An additional, novel part of the system are c.300 small, portable "QuickCheck" units which capture two plain index fingers, templates of which are extracted and transmitted via mobile phones (using a GSM network) to the central system where an automated search is conducted. An unverified result is sent back to the originating unit, normally in about five minutes. The templates are not retained.

ARC (Application Registration Card)

Added to the system has been an application to allow production of biometric identity cards containing, together with alphanumeric data, two index (usually) fingerprint templates stored in a 2k memory chip. Data from the IAFS record is used in the production process to avoid duplicate data entry. ARC records are stored in their own, partitioned database. The cards can be read and fingerprint checks against the cards conducted on all the QuickCheck units. A subset of the data held on the cards can be read at all main Post Offices in the UK for benefit payment purposes.

EURODAC

Practically all (there are a few exceptions) IAFS records are re-scanned on an interim standalone system and transmitted to the Eurodac system in Luxembourg. Here, an automated search is conducted against the database of nearly all EU immigration fingerprints to determine if a person has made a previous record or application in another European country. It is intended that direct connection will be made between IAFS and Eurodac in September. This will obviate the need for re-scanning. A further project is being initiated to allow identification of those who have been granted refugee status in Europe and, as a result, had their Eurodac record deleted but who then travel to the UK to register a further asylum claim.

VIAFS (Visa Immigration and Asylum Fingerprint System)

This is a pilot project which provides the biometric capture component at selected posts abroad (currently just Colombo, Sri Lanka) to enable index fingerprint capture and passport bio page scanning as part of the application process. Fingerprint data is then transmitted back to the UK for insertion into the IAFS database. This allows identification, at a later stage, of those who have a previous IAFS record and even those who destroy documents or will not admit even basic information such as name and nationality.

PIFE (Police/Immigration Fingerprint Exchange)

The aim of this project is to install a direct connection between IAFS and the national police fingerprint system (NAFIS) to allow cross checking as required. As an interim measure some cross checking utilising high-resolution fax machines is conducted and a small number of QuickCheck units have been issued to certain police units. Results to date indicate high “hit- rates”.

Reliability of the system

The IAFS system reliably identifies those who have previously been enrolled. The quality of records does depend on the skill of the officer taking the prints but is generally good and quality checks are a routine part of the process. Accuracy on the QuickChecks is not quite as high as LiveScan and CardScan and GSM communications are sometimes difficult, nonetheless users find them very helpful and, every day, they make useful identifications, sometimes very important ones that lead to the apprehension of criminals.

Reliability of the ARC application is still to be fully defined as usage of these cards increases. IND is one of the first agencies to issue biometric identity cards. Cards are produced at the biggest ports (Heathrow, Gatwick and Dover as well as certain other sites. Temporary “Conversion Centres” were also set up to allow applicants with the previous document to be issued an ARC.

It was quickly observed that devolved production was difficult because officers used the system infrequently and did not build up the necessary skill levels to deal with the minor but frequent problems that developed on the highly mechanical card printers.

Reliability of the cards themselves in benefit payment transactions has been fairly good. Card failures are occurring but at a low but persistent rate. ARCs are just beginning, at one pilot site, to be used in the reporting process. It is too early to assess performance in this process.

Conclusions and present situation
The Immigration Biometric Identification (IBI) Programme comprising all the projects above has enabled IND to have one of the most comprehensive biometric identification systems in the world. It allows fingerprint identification, production of biometric identity cards, cross checking with the biggest international biometric system, Eurodac, and, soon, direct cross-checking with the national police system. Additionally, the UK through the programme is one of the first countries to pilot the inclusion of biometric capture as part of the visa application process.

However, much remains to be done and in common with other countries major projects will need to be undertaken to fully realize the potential of biometrics for immigration control and travel security purposes.

— END —