Organization for Security and Co-operation in Europe

United States Mission to the OSCE

OSCE/ICAO Expert Workshop on Travel Document Security: From Basics to Biometrics

1 – 2 March 2004, Vienna, Austria

WORKSHOP REPORT

EXECUTIVE SUMMARY

The Organization for Security and Co-operation in Europe (OSCE) and the International Civil Aviation Organization (ICAO), with the extra-budgetary support from the Government of the United States, hosted the international expert workshop on travel document security on 1 and 2 March 2004 in Vienna. One hundred and forty-five experts from the OSCE participating States and ICAO attended the workshop, including travel document issuing and immigration authorities from 47 OSCE capitals, four of the OSCE partner for co-operation States, six partner organizations (EU, IOM, UNODC, Interpol, OECD and UNHCR), and representatives from four OSCE field operations. The event, organized by the OSCE Secretariat's Action against Terrorism Unit (ATU) in collaboration with ICAO, addressed a broad range of topics relating to travel document security. Invited presenters included experts participating in ICAO Working Groups (WG) on travel document issues, the International Organisation for Migration (IOM), the European Commission (EC), as well as national experts from Bulgaria, France, the former Yugoslav Republic of Macedonia and the United States.

The issue of travel document security was given particular importance by the 2003 Maastricht Ministerial Council of the OSCE, which adopted a Decision on Travel Document Security, reflecting commitments by OSCE participating States in implementing recognized international standards for travel document security. It also tasked the OSCE Secretariat to convene an expert workshop on implementation of the decision and assessment of the needs for related assistance.

The ATU, in close co-ordination with ICAO, subsequently undertook planning for this technical workshop involving travel documents experts. At this workshop, participants were presented with a comprehensive overview of the widely recommended international standards for handling and issuance of travel documents and the specifications and benefits of the Machine Readable Travel Documents (MRTDs). During the session on advanced technologies, participants were given presentations on the essence of applying biometrics to travel documents and the required security features, with examples of countries and regions with immediate future plans to implement this new technology to their ID and travel documents. With the examples from Bulgaria and the former Yugoslav Republic of Macedonia, participants were informed about the various concerns that might arise when states consider implementation of new security standards for their travel documents.

Overall, participants agreed that the workshop was very useful and informative, inspiring new initiatives and ensuring states' efforts to comply with international standards. The workshop served as an excellent forum for national travel document officials, the OSCE, the ICAO and other international organizations to exchange information and experience as well as initiate future co-operation.

REPORTS OF THE WORKING SESSIONS

Welcoming Remarks

The Chairman of the OSCE Permanent Council Ambassador Ivo Petrov welcomed the participants on behalf of the OSCE Chairmanship-in-Office. Recalling that fight against terrorism remains a tremendous challenge, he mentioned that it is among the top priorities of the current Bulgarian OSCE Chairmanship. The CiO has made counter-terrorism a continuing high priority for 2004. Ambassador Petrov underlined the importance of travel document security in preventing the movement of terrorists, as well as other cross-border criminal activities. He pointed out that the goal of the workshop was to contribute to the implementation of the decision of the Ministerial Council by raising awareness among participating States about the existing and developing standards concerning travel document security, outlining their future steps to meet the commitments defined by the Ministerial Council decision and, most importantly, to identify needs and possibilities for providing technical and financial assistance to those who may need it in order to fulfil their commitments.

In her welcoming remarks, **the Chairperson of the ICAO Working Group on Education and Promotion (EPWG)**, **Ms. Susan Jessop,** described ICAO's activities in the area of travel document security. She stressed the importance of efficient border control through the use of fraud resistant travel documents. Ms. Jessop underlined that the workshop would contribute to enhancing travel document security by impressing on participants the importance of identity safeguarding through a reliable process of entitlement determination, handling and issuance, as well as by considering new methodologies, standards, technologies and applications for travel documents production.

Mr. Brian Woo, Head of ATU, served as Moderator for the Opening Session and the Session One on Minimum Security Standards and MRTDs.

Session One: Minimum Security Standards and MRTDs

Mr. John Hotchner's presentation focused on **the Minimum Security Standards for the Handling and Issuance of Machine Readable Passports**, a key document which outlines various mechanisms for preventing staff fraud in the handling and issuance process, through variety of controls and identifying possible methods for internal fraud. The presentation covered a wide range of topics including the vulnerabilities of passport operations, advantages of automated systems and Machine Readable Travel Documents (MRTDs), need for senior management support in strengthening internal control and centralization vs. dispersed issuance. More importantly, Mr. Hotchner discussed recommended practices for each step in the passport handling and issuance process - passport handling, passport application and adjudication and passport issuance and delivery - as well as organizational and personnel issues. Furthermore, the presentation outlined the most important principles of internal control within the passport issuing and handling authorities, highlighting the importance of establishing clear procedural standards and the need to constantly be on the lookout for unrecognized vulnerabilities.

Ms. Muriel Sylvan spoke on the topic **Securing the Whole Chain of the Passport Handling Process**. Providing a comprehensive overview of France's ongoing efforts to remodel ID cards and travel documents facilities, she informed that France is undergoing a major project which will go beyond just introducing biometric technology to those documents. The plan focuses on establishing a single procedure for issuing ID cards and travel documents in line with recommended international standards, with the objective of simplifying the application process and maximizing documents security. France is in favor of introducing biometrics, as this will enhance applicant identification as well as reinforce security for issuance. Ms. Sylvan described the use of an electronic chip to store biometric data, which would ensure that documents are secure throughout application, issuance and handling, and mentioned that such technology is pending the EC's approval. The presentation outlined in detail France's future documents issuance procedure, starting from personal application at the state

hall and automated transfer of data to the central database using digitized photographs and fingerprints to centralized processing and personal pickup of the document. As an underlying principle for the entire process, it was noted that security of documents and protection of individual data should act as two equally important aims and be mutually beneficial and reinforcing.

Mr. John Mercer's presentation on **the Standard for Machine Readable Travel Document (MRTDs)** focused on the ICAO Document 9303, a suite of standards that describes the specifications for MRTDs which allow global compatibility and interoperability. Specifications are included for optional expansion of the machine readable capacity as well as machine assisted identity confirmation, and machine readable security features. In addition to detailing the structure of the Document, the presentation surveyed the history of the travel document standards, dating back to the days of the League of Nations, evolving through the 1963 UN Conference on Travel and Tourism, the establishment of ICAO Panel on Passport Cards and the approval of the first Document 9303, which then became the basis of the first machine readable passports. Through the establishment and work of the ICAO Technical Advisory Group (TAG) and Working Groups (WG) on MRTDs and the concurrent work done by the International Standards Organization (ISO), MRTD standards have been established as the major international reference point. In addition the TAG-MRTD's main role in establishing standards, maintenance of the standards, provision of technical assistance and advice to states and identifying and resolving problems with use of the standards, the OSCE/ICAO workshop on Travel Document Security was cited as an example of the TAG-MRTD's ongoing outreach programme.

Mr. Malcolm Cuthbertson opened his presentation on **Complexity of Modern Travel Documents** with an overview of the development of the travel document over the past 20 years. The presentation highlighted some of the complex decisions facing travel document issuing authorities and identified sources of international standards. Mr. Cuthbertson surveyed the various techniques for printing on the passport books used in the OSCE and other regions, ranging from laser engraving and pigmented ink to laser print and photographic printing technology. Noting that the decision to use a certain technology lies with the availability of resources for each state, he noted that if any conclusion could be drawn it was that the printing technology tends to gravitate along geopolitical profiles. The presentation also included additional security measures used by states, including biometrics. It was noted that governments' decisions regarding travel documents involve issues concerning central or decentralized issuance, personalization technology, levels of document and issuance security, and regional standards. Furthermore, the final decision or solution is an outcome of the combination of these and other elements. In conclusion, Mr. Cuthbertson noted that whereas there are numerous sources for information and advice, such as other governments and various ICAO WGs, every country is different in their issuance and security requirements, and it is important that states define such requirements first before deciding on the technology to be used.

In his presentation on **Photo Digitization and Implementation Considerations for Issuance, Dr. Otto Bernecker** focused on the responsibility of the passport issuing authority in securing the document's lifecycle. By doing so he raised issues concerning document-based identification, overall document security and quality management, as well as the advantages of facial identification and biometrics. When identifying an individual based on a travel document, three questions must generally be ascertained. The first question is whether the document presented is actually genuine, which can be done by providing a very distinct set of properties for the document, such as holograms. The second question is whether the data on the document is authentic, which can be ensured by physically protecting the data or by using cryptographic data protection schemes. The third question of how to link the document to the rightful bearer can be answered by providing distinctive biometric data on the document, such as a digitized photograph, a fingerprint, or an iris image. According to the presentation, the key to document security is the art of keeping variance within acceptable limits, preventing breaches of security in the handling and issuance process. A supervision system helps to optimize the work of the responsible parties. Optimization could be achieved by determining the degree and cause of deviations, then proposing measures to remedy the cause and adequately

readjusting target values. A division between the technical sections involved in the issuance process is an important aspect of quality management as it facilitates the supervision system.

Following the presentations there was a discussion on the minimum security standards and MRTDs. A question was raised about co-ordination at the national level among travel documents and border authorities, and the possibility of creating a centralized database. Experts recommended that travel document issuing authorities should take the lead in bringing together different units at the policy level in order to find ways to fight common threats, and noted that such co-operation is increasingly taking place among states as well as international organizations. However, it was noted that creating a centralized one-size-fits-all database would be very difficult.

In response to a question as to whether there is a plan to update the NTWG documents and recommendations in line with ISO standards, ICAO experts informed that the format for amendments to travel document specifications are to be discussed at the TAG plenary in May 2004.

Regarding the value of the traditional passport books if the biometric identity confirmation is used at border control checkpoints, experts underlined that the use of traditional passport books will continue as they enable a person-to-person check at border points and it will take time for people to have trust in the new system. Also, they serve more functions than an ID card. As an example, EU ID cards cannot function in the manner of a passport book, which can, for example, contain residence permits and other relevant information. In addition, these cards will not necessarily be globally interoperable, although bilateral agreements could be possible. It was also noted that as MRTDs are widely in use and many states cannot adopt the biometric technology immediately, the traditional passport book still has a long life.

In response to the questions about how the ICAO and participating States manage to reconcile the protection of privacy with the security standards intended to be applied in the documents, it was explained that only the biometric data already available in physical form should be included in the chip and must not be in a coded form on the document. To maintain transparency, it was emphasized, authorities must inform the owner of the biometric information of the scope of information to be included in the chip and the exact purposes of its use.

Regarding the issuance procedure of biometric passports for overseas citizens, Ms. Sylvan noted that in the case of France, the same security norms are used for all French passports, while France does not have a definitive answer as to emergency passport security standards and is currently discussing this issue. It was mentioned that applying the same biometric security features to passports issued for citizens abroad would be difficult. Citing the case of the US where 12-15% of all passports are emergency ones, it was underlined that the key to increasing security of these documents would be to make them valid for one year only and non renewable, although currently no common standards regarding the security of temporary passports are available. Some countries issue temporary passports in different colors to mark the distinction. It was pointed out that the standards proposed for the Emergency Passport will be presented at the TAG plenary in May 2004.

A question was raised as to how the ICAO or individual governments treat other travel documents, such as the Refugee Convention Travel Document, given the trend of higher security standards for national passports. ICAO experts explained that while such documents serve as valid travel documents, it is recommended that these documents are printed in line with other legitimate travel documents with enhancement of their existing standards.

Session Two: Advanced Technologies

Mr. Robert Mocny began his presentation on **the Enhanced Border Security Act and U.S. Visit Program** by outlining the four primary interests of the program as enhancing the security of U.S. citizens and visitors, facilitating legitimate travel and trade, ensuring the integrity of the immigration

system, as well as safeguarding the personal privacy of the visitors. The Visit Program has established a system to collect, maintain and share personal information on foreign nationals in order to determine whether the individual should be allowed to enter the U.S. Additionally, the system determines whether a foreign national can receive, extend or modify immigration status, has overstayed or otherwise violated the terms of their admission, should be apprehended or detained for law enforcement action, or needs special protection due to refugee status. It will establish a comprehensive view of border management that will eventually lead to a virtual border, a principle that exports the border checkpoint from the point of entry to the point of departure. The first major deadline of U.S. Visit is 26 October 2004 when the program is planning to deploy infrastructure capable of reading biometric machine-readable travel documents at air- and sea ports of entry. By this date, all countries exempt from an entry visa for the US must issue biometricly enabled travel documents following the ICAO standards. By the end of 2004, the 50 busiest land points of entry in the U.S. will also be equipped to read these types of travel documents. By the end of 2005 this entry procedure will be extended to the remaining land border points of entry.

Ms. Sylvia Kolligs focused her presentation entitled **Recent Developments in Document Security and Biometrics within the EU** on three legislative proposals that the EC has recently sent to the Council of the EU and the European Parliament. In the context of increasing border security, the EC has proposed that two biometric identifiers and a uniform format become standard both for Schengen visas and residence permits. The third proposal adopted by the EC concerns security standards and biometrics for EU passports. This overall initiative comes in response to the complex security situation, in particular travel document security, with the growing number of falsified travel documents. Concerning visas and residence permits, the first goal of the EC was to bring forward the final date for the introduction of a photograph in the visa stickers from 2007 to 2005. Overall, the EC regulations, subject to the opinion of the Parliament and adoption of the Council, provide for the eventual mandatory storage of the facial image as the primary biometric identifier, as well as an obligatory second biometric identifier, which should be the fingerprint. Both identifiers are foreseen to be captured on the travel document, as well as stored on the Schengen Information System (SIS), for “background checks”, or identification purposes. For EU passports, the EC has followed ICAO’s approach and introduced the facial image as the primary interoperable biometric identifier, but made the storage of a second biometric, such as fingerprints, optional.

In his presentation on **the New World of Biometrics in Documents**, **Mr. Gary McDonald** spoke about the way in which application of biometrics in documents has become so important, citing global interoperability and improved facilitation and security, as well as key national legislation, such as the US Enhanced Border Security Act, as the chief driving forces. He cited four key technologies required to achieve global interoperability of biometrics, which are: common data carrier, common data structure, common biometric and common security approach. The presentation also surveyed the current status of application of biometrics in travel documents, including the three biometrics in use (facial, iris and fingerprint), the image of the face is being singled out as the obligatory feature that is globally interoperable, with fingerprints or iris being the secondary, optional feature. On the key question of whether biometrics would be able to replace passports, Mr. McDonald noted that work is currently underway to enable sharing of passenger information in real time and that the minimum common standards need first to be met globally before such action can be considered.

Mr. Joel Shaw gave a comprehensive and thorough presentation on **the Essence of Biometrics**, outlining the various physical and behavioural biometrics in use and their key qualities and the essence of using biometrics in travel documents. Machine assisted identification confirmation, enabled by the application of biometrics, along with greater vigilance and more effective procedures, leads to improved, more secure identification. However, Mr. Shaw also noted the importance of creating a comprehensive global system to complement these technologies. Global standards are being established and maintained and other related issues dealt with through the collaborative work of the ICAO and ISO on MRTDs. Explaining that the facial image best matches the unique requirements defined by governments for travel and ID documents, and thus is the best biometric identifier for global interoperability. Mr. Shaw also noted that it supports co-existence with current generations of

MRTDs and also supports lookout identification capability. It was pointed out that the contactless chip best delivers facilitation and enhanced security, by way of encoded details written to chip following the Logical Data Structure. Recent testing in real world situations has shown that the new technology works well, proving to be a great improvement from some of the traditional methods of confirming identity. In conclusion, Mr. Shaw emphasized that biometric travel documents using facial images are compatible with current passports and can be introduced immediately with the option of adding secondary biometrics. Recognizing the existence of national legislation requirements which might prevent biometric technology, he reiterated that biometrics should be viewed as a set of standards that can be used as support tools by individual states according to their requirements.

Mr. Alain Bianchi presented **France's current activities relating to the use of biometrics in travel documents**. Mr. Bianchi noted that in addition to being an essential tool in fighting forgery and developing ideal security conditions for electronic administration of documents, biometrics also guarantee, through security protection of data, that personal information is not misused. Citing reasons for France's decision to adopt biometric features, Mr. Bianchi noted the recommendation by ICAO and the requirements of the EU, as well as the recognized need for harmonized standards for travel and ID documents and the global interoperability of biometrics. He informed that France plans to start a pilot project in late 2004 with the use of digitized photos in visas. It was noted that recognition error rate of the facial biometric is still rather high and for this reason biometrics should remain a tool supporting the traditional person-to-person recognition, rather than playing a primary role. To date, France views fingerprints as the only biometric identifier meeting the necessary criteria with low error rates and favors the inclusion of fingerprints in documents as a second biometric. Mr. Bianchi also touched upon the EU's plan for establishing an interoperable database, setting up a uniform infrastructure and integration of biometrics in documents.

Mr. John Davies's presentation on **Securing the Biometric** focused on the essence of securing biometric data through different encryption mechanisms, in particular **the Public Key Infrastructure (PKI).** The e-passport will initially contain biometric information, facial image (mandatory) and fingerprint and iris data (optional) as well as personal details from the passport bio-data page, initially enabling read-only access to the electronic data. Mr. Davies acknowledged the tension between ensuring the security of electronic data from inappropriate access and facilitating easy access to the electronic data by immigration authorities. He explained that, as an established method of protecting and authenticating data held on computer chips, the PKI scheme proposes a peer-based environment with each state exercising autonomy with respect to passport security and an agreed means of sharing and updating public keys. The presentation outlined responsibilities of states issuing and reading e-passports relating to protection of PKI and maintaining/disseminating up-to-date information about public keys. The ICAO is responsible to provide an efficient and reliable public key directory, ensure the directory is only updated by member states and provide open access to public key information to participating states and organizations. Mr. Davies also drew attention to the PKI Technical Report which proposes a technical framework and guidelines to enable each country to develop secure e-passports and includes an annex on PKI and security threats to aid individual states with their own risk analysis and mitigation decisions.

In the subsequent discussion session, participants actively raised questions regarding issues covered by the presentations on advanced technologies and biometrics. In response to questions regarding the US Visit Program, experts explained that while under the SEC 303 the US visa waiver countries should have in place the biometric capacity by the 26 October 2004, their citizens can still travel to the US with travel documents produced prior to this date. It was also noted that the US does intend to start producing passports with one biometric identifier and a new design by 26 October 2004.

In response to a question of whether there is a facial verification technology approved by the ICAO and ISO, experts mentioned the ISO SC37, which deals with technologies for global interoperability and establishes the best way to ensure that images and biometric data can be interchanged and globally interoperable. It was reiterated that in reality the ICAO bases its decisions on the work done within the ISO, thus helping to accelerate the implementation of ISO-approved standards.

Regarding the use of fingerprints as a biometric identifier and the way they are checked against the central database, Mr. Bianchi noted that France uses the one-to-many check, rather than one-to-one check. On the same issue, ICAO experts expressed the Organization's view that an exhaustive check is a very difficult task and governments will only start establishing such a system in the coming years, going through all the existing data available in their current systems.

Questions were raised about the ability of biometric technologies to adapt to human growth alterations and the possible replacement of the biometric system with a DNA system. In terms of facial images, it was explained, studies have shown that facial images of people over 18 years of age have stability and are thus reliable as biometric identifiers. Fingerprints of two-year-olds do not undergo further change, and iris as a biometric identifier is known to undergo least degradation. It was explained that the replacement of the biometric system with a DNA system would be a very expensive transition, although it should not be ruled out as a possible future option.

On a general note regarding the application of biometrics in travel documents, it was mentioned that a lot of financial resources are about to be invested in biometrics or contactless chips for enhancing the security of international travel. In this context, a question was raised as to whether any organization plans to carry out an independent scientific assessment of the benefits and limitations of the ICAO-recommended primary and secondary biometrics in real-life situations. In response, it was noted that current technology is changing very fast, and it is still up to every individual country to decide on the optimal technology best fitting their requirement. In case a state scientifically finds shortcomings of ICAO standards, it is encouraged to approach the ICAO to raise their concern. On the issue of the level of resistance of contactless chips, in relation to the 10-year validity of most passports, it was noted that independent scientific assessment is difficult and not available and that the May 2004 meeting of the ICAO TAG will consider such testing. It was additionally noted that a passport with a broken chip is still valid and can be used for travel, while international guidance is still to be worked on by ICAO WGs for such cases.

With reference to the ICAO recommendation of 'one person - one passport' policy, it was pointed out that many states issue family-unit passports, which raises the question as to how to include biometric features for children in family-passports. In response, ICAO experts clarified that family-unit passports are not compatible with the use of biometric identifiers and that it is recommended to issue separate passport for each person in the family. In this regard, it was additionally noted that having separate passports for children and requiring them to personally appear at application for travel documents also helps prevent children from being trafficked or their identities abused for terrorist purposes. On the validity period of passports, experts mentioned that states currently issue passports that are valid for five or ten years, with the five-year-valid passports having better performance rate.

A participant reminded that the OSCE Ministerial Decision commits all OSCE participating States to comply with the ICAO standards for handling and issuance by December 2004 and expressed the opinion that states need advice as to how they should go about updating their travel document systems and how best to get started evaluating their handling and issuance procedures against the ICAO standards. In response, ICAO experts outlined the first several steps. As a start, the existing documents should be evaluated against available standards, followed by securing executive-level support for funding and personnel resources for such upgrading. Equally important is the needs assessment by technical experts of concrete measures to be undertaken. It was also explained that possible technical and financial advice are available through different channels, including countries within regions that are advanced in their travel documents technologies, international organizations, such as ICAO and its WGs (e.g. EPWG) and private industry. OSCE participating States were also encouraged to consider participation in ICAO TAG meetings to discuss such assistance issues.

The need for ICAO's technical reports and handling and issuance procedures to be available in other languages, in particular in Russian, was pointed out as an obstacle for many states when it comes to implementation. ICAO experts acknowledged that it is ICAO's obligation to have these reports

translated but for speedy publication of these documents, they are often given waiver for translation into other languages. It was noted that this issue will be addressed with the appropriate offices in the ICAO. On a similar note, ICAO experts explained that the need for mechanisms for wide distribution of ICAO standard documents is currently under discussion by ICAO TAG, to ensure effective information flow to all the relevant authorities.

Session Three: Developing a National Strategy and Assistance Issues

Mr. Terry Hartmann gave a presentation titled **Getting Your Country's Documents in Line with International Standards – Developing a National Strategy**. He pointed out the importance of not rushing the implementation of biometrics but to carefully devise a strategy first. In this respect, he emphasized to always conduct a thorough threat analysis, identifying a country's weakest links regarding travel documents (such as documents issued abroad, etc). Mr. Hartmann addressed the passport book, covering printing techniques and relevant security features, including the Machine Readable Zone, Photograph Substitution and Logical Security Standards. Overall, however, he explained that securing the chain of passport handling process is the most important element, noting the human vulnerabilities during this process. While outlining several possible ways to best employ biometrics (identification, verification, authentication, and others), Mr. Hartmann underlined the necessity to always research new technologies in the context of one's own operation, in order to ensure efficiency and effectiveness and to avoid the wasting of resources. Moreover, he urged countries to constantly assess their technologies and beware of companies trying to obtain lucrative government contracts in the TDS sector. Particular emphasis was placed on ability of biometrics to prevent fraud, underlining the necessity of close co-operation between customs-, passports-, and immigration authorities as well as working to ensure not only local but also global interoperability.

Mr. Valery Spassov presented **Bulgaria's Experience in Introducing MRTDs with Digitized Photos**. In December 1997 Bulgaria decided to accelerate the replacement of ID documents for Bulgarians and foreigners living in the country and began preparations for introducing MRTDs with digitized photos as replacements. The project was assigned to the Ministry of Interior, which assembled an expert team, divided into working groups focusing on legislation, design and security features of the documents, definition of technical requirements, design and development, security issues and data protection, as well as quality management and staff training. Concerning management, it was decided that the National Population Register would be incorporated into the Ministry of Interior's identity document system. Thus, civic information, such as birth, marriage, death and name changes, is also accessible by the authorities issuing identity documents in Bulgaria. Additionally, it was decided that the previous practice of decentralized issuance would be maintained. All 18 types of Bulgarian state documents (such as ID cards, passports, visas, driving licenses, resident permits and refugee documents) have been designed as a common family of documents, possessing common as well as distinctive features. In 1999, sixteen months after starting the project, Bulgaria started issuing experimental documents. Standard replacement of passports began in 2000, with ID cards beginning in 2002. The new documents have digitized color photographs with an electronically captured signature. The uniform design within the family of documents increases their security and furthermore reduces the time necessary for scanning and processing.

Ms. Lidija Andrijevik presented **the former Yugoslav Republic of Macedonia's Plans for New Identity Documents**. Discussing the current issuance system, she mentioned that the country issues its passports, ID cards and driver licenses on standard paper with the data produced by a type writer. The photographs are attached manually, and at times given additional security through holograms, for example. The identification page is laminated and all pages are given a watermark. The reasons for upgrading the country's official document issuance system is not only to meet the growing demand for these documents, but also to enhance security features. This would also implement EU directives and ICAO standards, as well as reduce the number of false documents in circulation. The country~~'s~~ plans to have in place an integral system for new documents, with central civil and documents databases, central production and distributed data collection and documents delivery, and start

producing the new generation of documents, by 2005. The plan foresees using new technologies such as polycarbonate and laser engraving techniques, as well as digitized photos, fingerprints and signatures. Ms. Andrijevik mentioned as the key concern regarding this new plan the discrepancy between the state budget and the required resources to implement the international standards and the choice of the optimal technologies and security features. In conclusion, the three key areas for assistance needed were outlined: first, consultants are needed to assist in developing a national strategy; subsequently, expert advice will be necessary to find the optimal technology and security features fitting the national strategy; most importantly, she noted, financial assistance is needed to support the new system equipment and establishment.

Addressing **the Need for Technical and Financial Assistance: Implications in Light of the Maastricht Ministerial Council Decision on Travel Document Security, Mr. Charles Harns** presented the International Organisation for Migration's (IOM) primary role, namely to assist States in building of migration management capacities. He noted the strong basis for co-operation between the IOM and the OSCE, as 49 of the OSCE participating and partner States are members or associated with the IOM. It was also stated that the rationale for improving travel document issuance, border and related systems was to meet international norms for management of migration, to enhance routine security, to speed normal border crossings, to combat trans-national organized crime, as well as to combat terrorism. Identified as the most pressing needs were technical assistance to help prepare policies and to enhance the internal integration and external linking capability of existing systems. Giving examples of IOM's activities, such as assessment and border assistance in different regions, Mr. Harns noted that international organizations, such as the OSCE and IOM, should work toward programme frameworks that provide consistent support, over time, toward well-assessed goals, in particular in terms of comprehensive travel document creation, issuance, data linkage, and border management systems. Co-operation and co-ordination between concerned agencies and governments should also be increased. He also recommended that while prioritizing travel documents and border systems improvement, the "virtual borders", such as temporary travel documents often issued at Embassies or Consular offices, should not be neglected.

Concluding Remarks

Mr. Dimitar Jalnev from **ATU** indicated that a summary of the conference's full and ranging discussions would be provided to participants and experts within the next several weeks. He thanked the experts for their excellent presentations. Mr. Jalnev expressed gratitude to ICAO for its active role in developing the concept for the workshop and lining up leading international experts as presenters. He thanked also the US government for its generous contribution to make the workshop possible, as well as the OSCE participating States for sending the relevant national experts, which ensured useful and productive work. He also expressed appreciation for the OSCE Conference Services and interpreters for their dedicated support and closed the workshop.

Summary of Participants Evaluations

Overall, written participant responses were very positive, complimenting not only the speakers and their presentations, but also the general organisation and execution of the workshop. Multiple comments emphasized the workshop's necessity and usefulness, particularly with regards to inspiring new initiatives and ensuring their accordance with international standards. In this respect, several responses described the workshop as an excellent opportunity to liaise with ICAO experts, exchange experience and information as well as initiate future co-operation.

Demand was expressed for subsequent workshops to offer an even greater variety of topics and to increase focus on technical details as well as practical information from different immigration offices. Organizational suggestions for the future included the distribution of badges carrying participants' names and affiliations and to better cater for vegetarians during lunches.

Evaluation Results

Day One: Morning	Poor	Satisfactory	Good	Excellent
***Session 1*:** Minimum security standards for handling and issuance	**2**	**5**	**9**	**11**
***Session 2*:** Securing the whole chain of the passport handling process	**3**	**11**	**10**	**3**
Session 3: Benefits of machine readable travel documents (MRTDs)	**2**	**6**	**9**	**10**
Session 4: Printing techniques and security features	**2**	**6**	**10**	**9**

Day One: Afternoon	Poor	Satisfactory	Good	Excellent
***Session 5*:** Photo digitization and implementation considerations for issuance	**2**	**7**	**10**	**2**
***Session 6*:** Discussion and questions session on minimum security standards and MRTDs	**1**	**4**	**17**	**4**
Session 7: Presentation on the Enhanced Border Security Act and US VISIT Update	**2**	**3**	**15**	**7**
***Session 8*:** Presentation on recent developments in document security and biometrics within the EU	**4**	**9**	**7**	**2**

Day Two: Morning	Poor	Satisfactory	Good	Excellent
***Session 1*:** The new world of biometrics in documents	**2**	**4**	**14**	**7**
***Session 2*:** The essence of biometrics	**2**	**3**	**6**	**16**
Session 3: Pilot experiments relevance to the introduction of biometrics in travel documents	**7**	**8**	**7**	**4**
Session 4: Securing the biometric	**1**	**3**	**10**	**2**
***Session 5*:** Discussion and questions session on biometrics	**2**	**5**	**13**	**3**

Day Two: Afternoon	Poor	Satisfactory	Good	Excellent
Session 6: Getting your country's documents in line with international standards	**2**	**1**	**6**	**10**
***Session 7*:** Presentations on needs, technical and financial assistance	**0**	**7**	**1**	**4**
***Session 8*:** Discussion on developing a national strategy and assistance issues	**3**	**3**	**7**	**4**

Both Days	Poor	Satisfactory	Good	Excellent
The overall value of the workshop	**0**	**5**	**10**	**12**

Both Days	Poor	Satisfactory	Good	Excellent
The overall comfort of the workshop (venue, catering etc)	**0**	**0**	**8**	**19**

Total number of returned evaluation forms: 27