**ТЕХНИЧЕСКАЯ КОНСУЛЬТАТИВНАЯ ГРУППА
ПО МАШИНОСЧИТЫВАЕМЫМ ПРОЕЗДНЫМ ДОКУМЕНТАМ**

Пятнадцатое совещание

(Монреаль, 17–21 мая 2004 года)

Пункт 3 повестки дня. Доклад Рабочей группы по новым технологиям (NTWG)

ОБНОВЛЕННАЯ ИНФОРМАЦИЯ О РАЗРАБОТКЕ ТЕХНИЧЕСКОГО ДОКЛАДА ПО ОБМЕНУ ИНФОРМАЦИЕЙ МЕЖДУ ДОГОВАРИВАЮЩИМИСЯ ГОСУДАРСТВАМИ В ОТНОШЕНИИ УТЕРЯННЫХ, УКРАДЕННЫХ И НЕДЕЙСТВИТЕЛЬНЫХ ПРОЕЗДНЫХ ДОКУМЕНТОВ

(Представлено Рабочей группой по новым технологиям (NTWG))

1. ВВЕДЕНИЕ

1.1 На совещании TAG-MRTD/14 было утверждено предложение о дальнейшем выполнении NTWG работы, связанной с исследованиями и разработками в области организации в глобальном масштабе обмена информацией об утерянных, украденных и недействительных паспортах, включая подготовку по этому вопросу всеобъемлющего технического доклада.

1.2 В рабочем документе TAG-MRTD/14-WP/10 приводится описание результатов предварительных исследований, проведенных NTWG. Основное внимание в этом документе уделено вопросу организации обмена в глобальном масштабе данными об утерянных, украденных и недействительных паспортах путем использования существующей инфраструктуры базы данных Международной организации уголовной полиции (Интерпол) об украденных проездных документах (STD). За прошедший после этого период NTWG подготовила проект соответствующего технического доклада.

2. КРАТКАЯ СПРАВКА

2.1 В техническом докладе приводится дополнительная информация об обосновании организации и вариантах обмена в глобальном масштабе данными об утерянных, украденных и недействительных паспортах, при этом основное внимание уделяется использованию инфраструктуры Интерпола в качестве наиболее предпочтительного подхода к решению этого вопроса.

2.2 После TAG-MRTD/14 Интерпол продолжал заниматься разработкой и внедрением своей политики и инфраструктуры с целью создания глобального узла связи для государств-членов, чтобы обеспечить включение в свою базу данных дополнительных национальных данных об утерянных,

украденных и недействительных проездных документах, а также обеспечить доступ к таким данным другим государствам в реальном масштабе времени. Интерпол принял ряд резолюций, которые призваны обеспечить возможность непосредственного доступа к информации пограничным контрольным учреждениям, и доработал свою инфраструктуру средств связи I 24/7 в целях упрощения и автоматизации процесса включения дополнительных данных и предоставления доступа к ним. Эти меры позволят государствам-членам как вносить дополнительные данные в централизованную управляемую базу данных Интерпола, так и вести свою базу данных, предоставляя доступ к ней другим государствам путем использования сети средств связи Интерпола.

2.3 В техническом докладе для участвующих государств приводится описание обзора решений, а также информация об оперативной политике, технических вопросах и национальных требованиях. В этот доклад предстоит включить дополнительные определения технических требований протоколов.

2.4 В техническом докладе рекомендуется, чтобы государства-члены одобрили решения Интерпола в отношении организации обмена информацией об утерянных, украденных и недействительных проездных документах в глобальном масштабе.

3. ДЕЙСТВИЯ TAG-MRTD

3.1 NTWG предлагает TAG-MRTD:

a) принять к сведению содержание проекта технического доклада (распространен отдельно); и

b) утвердить предложение о продолжении проведения исследований и разработок в целях дальнейшей доработки технического доклада и включения в него подробных оперативных и технических требований, касающихся участия государств в системе Интерпол I 24/7.

– КОНЕЦ –

INFORMATION SHARING BETWEEN CONTRACTING STATES IN RELATION TO LOST, STOLEN AND INVALID TRAVEL DOCUMENTS

ICAO NTWG

TECHNICAL REPORT

Version 2.0

CONTENTS

1. Documentation History 3
2. Scope and Purpose 3
3. Introduction 4
Rationale for sharing lost, stolen or invalid travel document data 4
Outline of benefits and requirements of participation in real time data exchange 4
4. Solution Overview 5
Interpol 5
Bi-lateral arrangements 7
Other Options 7
5. Policy 7
Policy Overview 7
Legislative requirements 7
Privacy 8
Multilateral agreements 8
Costs 8
Access to databases 9
Integrity of data, modification of data 9
Enforcement and action on recovery 9
6. Technical Issues 10
Technical overview 10
7. National Database Requirements 11
Issuance Authorities 11
Border Control Authorities 11
Nations without central or linked databases 11
Standard data sets and formats 12
Blank Documents 12
Security Protocols 12
Standard document type codes 12
Country codes 12
System User Guides 12
8. Recommendations 12
9. Glossary 13

1. Documentation History

Date	Revision	Action
February 2004	1.0	Initial draft including conceptual operational model
May 2004	2.0	Updated version incorporating feedback from the NTWG meeting in The Hague

2. Scope and Purpose

The ICAO New Technologies Working Group (NTWG) has, as a work item, undertaken research into the opportunities for an electronic global interoperable data interchange in relation to lost, stolen and invalid passports. At TAG-MRTD/14 (Montreal 6-9 May 2003) Working Paper WP10 outlined the research undertaken and sought approval to develop a technical report on the preferred options/solutions available to states that may wish to make their national data relating to lost, stolen and invalid travel documents available to other states in electronic form for real time border control purposes.

The TAG approved further research and the development of a technical report that focuses on the solution offered by enhancing access to the existing INTERPOL Stolen Travel Document Database (STD) while allowing for independent bi-lateral arrangements between states.

This technical report provides guidance to states wishing to participate in a real time electronic globally interoperable data interchange of lost, stolen and invalid travel document details.

The report does not canvass all options for this type of data sharing however provides a methodology to use a similar infrastructure to that proposed to enable states to share data bi-laterally.

The report assumes that member states wishing to access data in a real time environment have, databases of lost, stolen and invalid travel documents, an electronic infrastructure at border checkpoints and an ability to create, maintain and connect to secure national and international networks.

The report recognises that not all member states will have the electronic and communication infrastructures in place to be able to take advantage of all of the functionality proposed however it is not intended to discourage states from

participating at least in the provision of data relating to their lost, stolen and invalid travel documents through existing channels.

3. Introduction

Internationally border control authorities are seeking timely and accurate information concerning the validity of travel documents presented at their borders. One of the key elements in determining validity is having access to data relating to lost, stolen and invalid travel documents.

Rationale for sharing lost, stolen or invalid travel document data

There has been long term acceptance that the global interchange of information on lost, stolen and invalid travel documents is a key risk mitigation strategy in relation to border control and identity theft. States are now commonly able to identify the use of their own lost, stolen and invalid travel documents when presented at their national borders however cannot access this information on those documents issued by other states to anywhere near the same degree. Global interchange of this information can provide benefits in the following areas;

a) Improved border integrity through the interception of passengers travelling on lost stolen or invalid documents

b) Identification of identity theft either at the border or in other situations where travel documents are presented as forms of identification

c) Improves the chances of identification of terrorist operatives travelling on false documents

d) Improves the chances of identification of criminal activity including people smuggling

e) Aids the recovery of national documents

f) Having global systems in place inherently limits the value and or use of lost, stolen or invalid documents for illegal purposes

Outline of benefits and requirements of participation in real time data exchange

It is envisaged that all participating member states, that have border control systems supported by an electronic infrastructure, will be able to improve border integrity through the identification of passengers (from all other participating member states) travelling on lost stolen or invalid documents prior to boarding (where APP type systems are in operation), in-flight (where API systems are in operation) or as they pass through border control checkpoints (land, air or sea).

Participation will require states to maintain an up to date database of lost, stolen and invalid travel documents and have this data available for high volume polling via an international VPN network. Alternatively states may electronically provide a list of these documents for inclusion in the INTERPOL database and update these lists on a regular basis.

Additionally states may wish to provide a 24/7 contact centre to support telephone enquiries from international border control agencies given that data-base information may not be sufficient to positively identify a traveller.

4. Solution Overview

Interpol

Since 2002 INTERPOL has operated a global centralised database of stolen and invalid passports. Initially this database was centred on the recording of stolen blank passport books with individual states manually keying information into the database via their national crime bureaus. The resultant international database has traditionally been only available to policing agencies in each member state.

Over the last twelve months there have been four key developments, which pave the way for, more efficient and effective use of lost, stolen and invalid travel document data. These are;

- General assembly agreement to extend access, where agreed nationally, from policing organisations to also include other agencies responsible for border control
- The upgrade and implementation of communication systems and protocols utilising secure Internet VPN technology for current users (I-24/7)
- The functionality has been deployed to enable member states to add data to INTERPOL's lost stolen or invalid document database without the need for physical keying.
- The development of the INTERPOL server infrastructure that will allow real time high volume polling of the INTERPOL database and or redirect queries to member states national databases of lost stolen or invalid travel documents.

At the 72nd INTERPOL General Assembly (29 September to 2 October 2003) Resolution No AG-2003-RES-04 was adopted. This resolution covers the rules around the processing of information for the purposes of international cooperation.

Effectively this resolution allows National Crime Bureaus (NCB's) to negotiate and implement agreements, for access to data relating to lost, stolen and invalid travel documents, with other national government agencies, in this case passport issuance and border control authorities.

The I-24/7 system is a global communications network hosted by INTERPOL. It currently allows Policing organisations from member nations to access the various INTERPOL central databases through secure VPN infrastructures. Using this system, Interpol National Central Bureaus (NCBs) can search and cross-check data in a matter of seconds, with direct and immediate access to databases containing critical information (Notices, stolen motor vehicles, stolen/lost travel and ID documents, stolen works of art, payment cards, fingerprints and photographs, a terrorism watch list, a DNA database, international weapons tracking and trafficking in human beings-related information)

INTERPOL has completed the roll out of its I-24/7 system to one hundred member states with the remainder to be completed in 2004. This system, based on EDIPOL data exchange protocol (a derivative of UN/EDIFACT), not only enables national crime bureaus to access INTERPOL data in real time but also has the facility to receive data directly from national databases e.g. lost, stolen and invalid travel documents databases held by issuance or other border control agencies.

INTERPOL has built a server infrastructure that connects to but is separate from its databases that will provide the hardware and software for border control agencies to poll against when a passport is presented. To handle the performance issues (millions of queries per day), an index-server will be deployed. This index-server « crawls » the external databases maintained by states, and builds an index database (without the data). This crawling can be done permanently to guarantee an up-to-date index. When INTERPOL receives a query, a yes-no response is generated, using only the index. In the case of a yes a second request is automatically sent via the I-24/7 network directly to the country of issue or in the case of states without their own server the INTERPOL database of lost, stolen and invalid travel documents. This is similar to the processes used by search engines like Google on public Internet.

These developments have created the technical environment at INTERPOL to propose a solution that will operate broadly as follows;

State *x* creates a database of lost, stolen and invalid travel documents. A standard subset of data is placed on an external server connected via VPN to the Internet.
A passport holder from state *x* presents their passport at the border control point in state *y* (at check in for APP and API). The passport is machine read and a message automatically generated via the I-247 system to the INTERPOL index-server. A yes-no response will be generated instantly. In the case of a yes response the query will be diverted to the travellers national server and a standard set of data returned within seconds. Given the data set matches with those elements of the document presented the traveller will then referred for secondary/further processing.

Alternatively nations may choose simply to provide formatted lists of lost and stolen travel documents electronically to INTERPOL. This would require an initial upload of existing data and regular electronic additions to listings.

Bi-lateral arrangements

The INTERPOL solution can be applied to bi-lateral agreements as part of the functionality of the I-247 system. This enables states to select/limit the access to their data however this is not the intent of a globally interoperable system.

Alternatively states wishing to enter into bi-lateral arrangements can potentially use the same communication protocols, data sets, policies and standards as those developed within this report. This would enable states that have databases available for polling through the I-247 VPN to a single server that can also be accessed directly with partner states. Partner states may be able to access a broader set of data elements to aid traveller identification.

Other Options

It is acknowledged many states do not have the electronic infrastructure to enable full participation in the solutions described above however existing paper based methodologies can continue to be successfully used as can databases already established by border control authorities.

It also recognised that there are a number of parallel or similar initiatives both regional and international being developed in a variety of fora. While these initiatives generally support the use of INTERPOL data or bi-lateral exchanges they are focused on broader issues (e.g. exchange of intelligence) rather than just lost and stolen documents.

5. Policy

Policy Overview

The three key policy objectives are to:

- Ensure, that states can legally publish data relating to its citizens and at the same maintain the privacy of those citizens
- Ensure, the integrity and security of data
- Enable, the real time global interchange of data

Legislative requirements

Although the solution does not call for the disclosure of travel document holders bio-data the fact that details of documents relating to them will be disclosed means that states may need to gain legislative mandate to allow international access to elements of their citizens travel document information. Any legislative amendments should cover issues such as:

- Collection and storage of data
- Privacy provisions including security
- Authorisation for dissemination to the international community
- Data lifecycle and non-repudiation

Privacy

Privacy is a key issue for states wishing to participate in the global interchange of data through the INTERPOL I-247 system and associated infrastructure. Most states have some form of privacy legislation and this will govern the extent to and the way states participate.

As a principle the minimum data to, enable the unique identification of a lost, stolen and invalid travel document will be available for interchange.

A standard data set has been developed (see technical issues) for interchange between the issuing and receiving states. This data set focuses on document details and therefore no name or other personal details have been included. This still may require action under privacy legislation (e.g. a privacy impact assessment) to carried out. It also may mean that issuing states will need to be contacted by receiving states in situations where the identity and biographical data of the original holder needs to be established or checked against the person presenting the document.

To ensure privacy and integrity of data only the issuing authority will be able modify data, however it should be recognised that when a lost, stolen and invalid travel document is identified that the data obtained via the INTERPOL solution will be retained by the receiving state.

Multilateral agreements

Nearly all ICAO member states are also members of INTERPOL. Effectively this means that a set of governance protocols for international data sharing are already in place and therefore once states have agreements in place between appropriate border control agencies and their national crime bureaus the need for separate multilateral agreements should be eliminated.

Costs

In general the user pay principle will apply.

The costs associated with hosting and operating the I-247 and related server infrastructure will continue to be met by INTERPOL. Participating states will be required to fund their own databases/servers and communication costs in a similar manner to that of their NCB's

Access to databases

INTERPOL'S governance structure requires that National Crime Bureaus (NCB's) control access to the I-247 and other systems.

All user agencies including issuance authorities will be required to negotiate and implement agreements, for access to data relating to lost, stolen and invalid travel documents. These agreements will not only include governance rules but also the technical infrastructure to be applied. INTERPOL has a memorandum of understanding (MOU) template for this purpose however national protocols will need to be established to develop roles and responsibilities for ensuring the integrity of data.

Data supplied and or made available by member states remains in the originating states control. The I-247 systems enable states to determine which other states can access data. It is expected that data relating to lost, stolen and invalid travel documents will be made widely available however it is recognised that states may want exclude others for a variety of political or security reasons.

Integrity of data, modification of data

Issuance authorities are responsible for the integrity of data published on their national servers.

As information is updated in national travel document issuance and or/lost, stolen and invalid document systems in real time particularly in relation to lost and stolen documents updating will be required on at least a daily basis. Additionally most stolen documents that are fraudulently presented without significant modification are used within 48 hours strengthening the case for regular updating

Only issuance authorities can modify and update data. While it would be useful if issuing states could automatically be notified if a document is recovered this will occur as a separate communication using existing protocols.

The proposed solution is based on the premise that polling will be by individual document and will occur at the border control point (at check in for APP and API). It does not envisage, nor will it be technically possible for states to build large composite databases from the information held on other national servers.

Enforcement and action on recovery

The key risk for states in providing global access to lost, stolen and invalid document data is that innocent citizens may be inconvenienced, refused entry or held in custody due to inaccurate data, incorrect identification or because they travel on documents previously reported lost.

While receiving states have the sovereign right to determine what action will be taken as a result of a positive return on a database query issuing states will want assurance that this action will not be judgemental and extreme.

No significant enforcement action should be undertaken unless the identity of the holder is certain. If uncertainty exists the receiving state must contact the issuing authority to establish if the person presenting the document is the rightful holder.

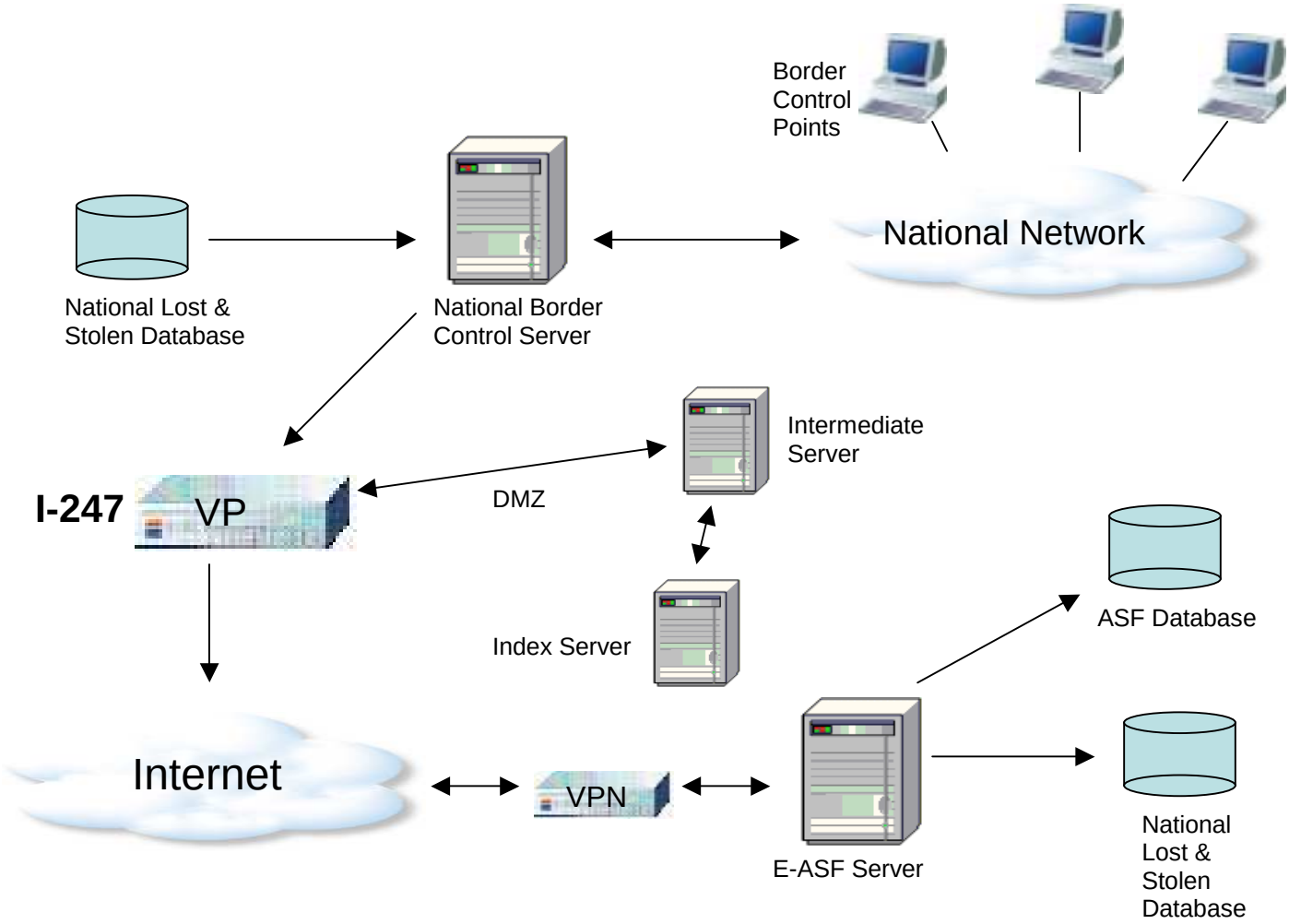
This will require issuing state to have the capability to handle such enquiries on a 24/7 basis.

Recovered documents should be returned to the issuing state using existing operational protocols

6. Technical Issues

Technical overview

The diagram below illustrates how the system will operate:



Business Flow

The business flow utilises standard business-to-business Internet processes.

Dependant on infrastructure, border control points query the national server which in turn queries the national database, and the international data base (e-ASF).
The connection between the National Server and the e-ASF uses the secured I-247 network.
E-ASF server queries the e-ASF database (extract of the ICIS), and queries external national servers.

To avoid direct link between the servers, a Demilitarized zone (DMZ) is used to guarantee the gap. The National Server transacts with the intermediate server in the DMZ. This intermediate server transacts with e-ASF. With this mechanism, it is impossible to have an access from e-ASF to the National Server. The DMZ functionality is fully compliant with the existing I-247 architecture.
At the national level, the national server publishes the information in an intermediate server placed in the DMZ of the I-247 VPN.
This publication is fully controlled at the national level; the country can select the information for publishing, control the integrity of this information, and control the access to this information.
The index server transacts directly with the e-ASF

7. National Database Requirements

Issuance Authorities

Many states have existing databases of lost, stolen and invalid documents or have the ability to extract this information from person centric issuance databases.

Publishing an extract from these databases will require the installation of web server/s or the communication infrastructure to enable the regular upload of data to the INTERPOL database.

The exact nature of this process will be the subject to INTERPOL guidance

Border Control Authorities

Many border control agencies currently have the functionality in their systems to interrogate databases within their internal networks and some have this functionality in relation to external databases. The INTERPOL solution would be an additional business-to-business linkage

The exact nature of this process will be the subject to INTERPOL guidance

Nations without central or linked databases

INTERPOL will continue to host a lost, stolen and invalid documents database for policing functions and to support states without the volume or infrastructure warrant maintaining their own server. States can load data by keying if required and will have the ability to poll the data of other participating states.

Standard data sets and formats

To ensure simplicity, maintain individual privacy and at the same time guarantee the uniqueness of records the following data elements have been selected

Data Element	Format	Example
Country Code	Three letter code	NZL
Document Type		P or V
Document Number	Alpa numeric	AA 005000
Date Of Issue	ICAO date format	010104
Date Of Expiry	ICAO date format	010114
Document Status	Prescribed list	Lost, Blank, Stolen

While most of data elements are self-explanatory the “Date of Issue” element is required as a number of states allocate a passport number to an individual and this is reused at each renewal.

Blank Documents

As blank documents may not have document numbers allocated and will not have dates of issue

Security Protocols

The I-247 system encrypts all information exchanges. Security protocols are based on an IPSEC, 3DES 128 bit encryption.

Standard document type codes

Standard ICAO type codes are to be used

Country codes

Standard ISO/ICAO three letter codes will be used

System User Guides

While there is a user guide in place for the I-247 system this will need to be amended and updated to provide for the enhanced system

8. Recommendations

The NTWG recommends that ICAO adopt INTERPOL as the primary infrastructure provider to enable the global interchange of lost stolen and invalid travel documents.

9. Glossary

Invalid travel document	A genuine passport or other travel document that has been issued incorrectly, as a result of fraud or has been recalled by the issuing state
EDIPOL	A data format standard
APP	Advanced passenger processing
API	Advance Passenger Information
Polling	In this context sending a electronic request to a database
VPN	Virtual private network
e-ASF	Electronic Automated Searching Facility
ICIS	Interpol Criminal Information Systems
DMZ	Demilitarised Zone
GS	General Secretariat