International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/17
13/9/05
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Sixteenth Meeting

(Montreal, 26 to 28 September 2005)

Agenda Item 2: Implementation of e-Passports
Agenda Item 2.1: Progress and Issues

UPDATE ON THE DEVELOPMENT OF A TECHNICAL REPORT ON INFORMATION SHARING BETWEEN CONTRACTING STATES IN RELATION TO LOST, STOLEN AND REVOKED TRAVEL DOCUMENTS

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 Since TAG/MRTD-13 in 2002 the NTWG has undertaken research on preferred options/solutions available to States that may wish to make their national data relating to lost, stolen and revoked travel documents available to other States in electronic form for real time border control purposes.

1.2 TAG/MRTD-15 (2004) approved the continuation of the on-going research and development work being carried out by the NTWG on the global interchange of information in relation to lost, stolen and revoked travel documents. The TAG/MRTD approved further development of the Technical Report to include the full operational/ technical requirements for participation by States in the INTERPOL global interchange system on lost, stolen and revoked travel documents.

1.3 Since that time the Technical Report has been refined to include operational/ technical requirements for participation by States in the INTERPOL global interchange system on lost, stolen and revoked travel documents. Version Five (5.0) is presented at this meeting.

2. SUMMARY

2.1 In many aspects version five (5.0) of the Technical Report is essentially unchanged from version two (2.0) presented at TAG/MRTD 15. The key changes reflect the evolution of the technical overview and the addition of Standard Operating Policies and Procedures (SOPPS) as an appendix provided by INTERPOL.

2.2 The Technical Report now provides sufficient information for States that are considering participation in the INTERPOL global interchange system on lost, stolen and revoked travel documents to make an informed judgement on the issue. The Technical Report does not attempt to provide a complete technical description of the connections to the I 24/7 system, as this information is not in the public domain. As the Technical Report indicates States wishing to participate should contact INTERPOL directly.

2.3 During the development of the Technical Report, member States had raised issues in relation to the capacity and reliability of the system. These concerns focus on the reliability of the Internet when using it for high volume real time processes and response times given the potential for millions of queries per day being channelled through the INTERPOL system. In response to this and UN Security Council Resolution Nr. 1617, from 29/07/2005 (which further urges states to share information, including that related to lost and stolen passports, in the fight against terrorism) INTERPOL continues to develop the infrastructure around the Automated Search Facility for Lost/Stolen Travel Documents (ASF STD) and as a result will be rolling out an evolved design towards the end of 2005. As yet the Technical Report does not incorporate these design enhancements. Broadly, this evolved design addresses the issues of reliability and volume by placing a mirror image of the central database in each member state, that will be accessible by border control agencies.

2.4 Until the latest design changes are available to users in an operational environment the Technical Report will not be further updated.

3. ACTION BY THE TAG/MRTD

3.1 The TAG/MRTD is invited to:

a) note the content of the draft Technical Report; and

b) approve the continuation of the on-going research and development work to further update the Technical Report as ASF STD design evolves and is available to member States in operational mode.

— — — — — — — —

WP/17 Attachment, Revised

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

ICAO NTWG

TECHNICAL REPORT

Version 5.0

CONTENTS

1. Documentation History 5
2. Scope and Purpose 5
3. Introduction 7
Rationale for sharing lost, stolen or revoked travel document data 7
Outline of benefits and requirements of participation in real time data exchange 8
4. Solution Overview 9
INTERPOL 9
Bi-lateral arrangements 14
Other Options 14
5. Policy 15
Policy Overview 15
Legislative requirements 15
Privacy 16
Multilateral agreements 17
Costs 17
Access to databases 18
Integrity of data, modification of data 19
Enforcement and action on recovery 20
6. Technical Issues 22
Technical overview 22
7. National Database Requirements 23
Issuance Authorities 23
Border Control Authorities 24
Nations without central or linked databases 24
Standard data sets and formats 25
Blank Documents 26
Security Protocols 26
Standard document type codes 26
Country codes 26
9. Glossary 27
Appendix 1 29

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
June 2004	3.0	Minor changes after Interpol feedback during TAG 15
May 2005	4.0	Major revision following the insertion of technical detail from INTERPOL
June 2005	5.0	Updated version incorporating feedback from the NTWG meeting in Lyon

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 revoked 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 revoked 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 revoked 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 revoked 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 revoked 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 revoked travel documents.

Rationale for sharing lost, stolen or revoked travel document data

There has been long-term acceptance that the global interchange of information on lost, stolen and revoked 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 revoked 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 revoked 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 revoked 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 revoked 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 revoked 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 revoked 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 two years there have been a number of key developments, which pave the way for, more efficient and effective use of lost, stolen and revoked 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 revoked 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 revoked travel documents.
- Resolutions and recommendations adopted by G8 Ministers, European Union (EU) and Organization for Co-operation and Security in Europe (OSCE), requesting their member countries to share their lost/stolen travel documents data with Interpol
- Resolution No. 26 adopted by the General Assembly held in Cancun, Mexico, October 2004.
- Recommendation to co-ordinate all regional initiatives to bolster the use of the Interpol System

- Resolution prepared by Japanese Ministry of Foreign Affairs representatives within the APEC Counter Terrorism Task Force, to be adopted by APEC Group, requesting all APEC members to share their lost/stolen travel documents data with Interpol

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 revoked 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, or decentralized 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 nearly all of its 182 member countries with the remainder to be completed in 2005.. This system, 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 revoked 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..

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 revoked 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 database of lost, stolen and revoked travel documents of State *x* (in the case of a state that does not have its own data on an external server query is forwarded to the e-ASF server at the INTERPOL General Secretariat (GS). A yes-no response will be generated. In the case of a yes response 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 revoked 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 revoked travel document is identified that the data obtained via the INTERPOL solution will be retained by the receiving state.

As defined in the INTERPOL Standard Operating Policy and Procedures (SOPPs) guidance material (see appendix 1)

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 revoked travel documents. These agreements will not only include governance rules but also the technical infrastructure to be applied. INTERPOL has a "Letter of Commitment" 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 revoked 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.

As defined in the INTERPOL Standard Operating Policy and Procedures (SOPPs) guidance material (see appendix 1)

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 revoked 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 states building large composite databases from the information held on other national servers.

As defined in the INTERPOL Standard Operating Policy and Procedures (SOPPs) guidance material (see appendix 1)

Enforcement and action on recovery

The key risk for states in providing global access to lost, stolen and revoked 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.

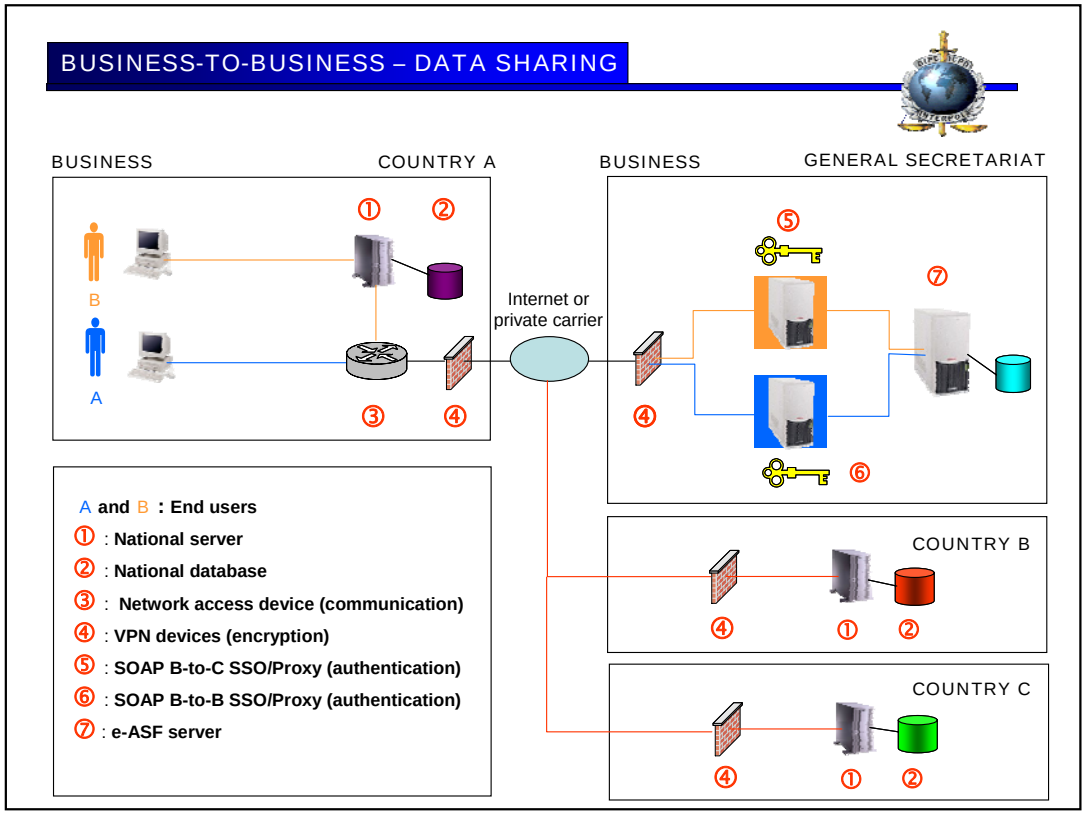
Recovered documents should be returned to the issuing state using existing operational protocols

As defined in the INTERPOL Standard Operating Policy and Procedures (SOPPs) guidance material (see appendix 1)

6. Technical Issues

Technical overview

Illustration of a BUSINESS-TO-BUSINESS database sharing model



Both *Business-to-Client* and *Business-to-Business* users can take advantage of the *database sharing* process

User "**B**" (*Business-to-Business*) dispatches a query to his national server "**1**" hosting a national database "**2**"
National server "**1**" automatically forwards the query to GS via the network access device "**3**"
The query is encrypted with the VPN devices "**4**"
User "**B**" is authenticated via the *HTML Business-to-Business Single Sign One server* at GS "**5**". The query is forwarded to the e-ASF server at GS "**7**" or to the national databases located in countries "**B**" or "**C**" depending on which country has issued the travel document.
The same forward process can be applied for a query sent by user "**A**" via the HTML *Business-to-Client Single Sign One server* "**6**"

7. National Database Requirements

Issuance Authorities

Many states have existing databases of lost, stolen and revoked 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 dependant on a states current issuance agency technical infrastructure. States integration into this system is a matter for direct discussion with Interpol

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 dependant on a states current border control technical infrastructure. States integration into this system is a matter for direct discussion with Interpol

Nations without central or linked databases

INTERPOL will continue to host a lost, stolen and revoked 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 A second alpha character may be present
Document Number	Alpha numeric	AA 005000
Date Of Issue	ICAO date format	010104
Date Of Loss/Theft	ICAO date format	010114
Document Status	Prescribed list	Lost Blank, or Stolen Blank, or Lost Issued, or Stolen Issued or Revoked

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. All data elements are mandatory. Document status data will be codified in line with Interpol protocols.

As defined in the INTERPOL Standard Operating Policy and Procedures (SOPPs) guidance material (see appendix 1)

Blank Documents

As blank documents may not have document numbers allocated and will not have dates of issue. Where the document has no pre-assigned Issuance number then a stock control is to be inserted.

Security Protocols

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

Details of Security protocols are available directly from Interpol

Standard document type codes

Standard ICAO type codes are to be used

Country codes

Standard ISO/ICAO three letter codes will be used

9. Glossary

Revoked 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
ASF-STD	Automated Search Facility for Lost/Stolen Travel Documents
ICIS	Interpol Criminal Information Systems
DMZ	Demilitarised Zone
GS	General Secretariat
Document Status: “Revoked”	A genuine travel document that has been obtained by fraudulently

Appendix 1

Automated Search Facility for Lost/Stolen Travel Documents (ASF STD)

Standard Operational Policy and Procedures for the Use of ASF-STD

Table Of Contents

DEFINITIONS…….. 3

PREAMBLE……. 4

PURPOSE AND FUNCTION……. 5

DATA INPUT REQUIREMENTS ……. 5

DATA PROCESSING……..6

DATA TRANSFER…….. 6

DATA ACCESS……8

RIGHTS AND OBLIGATIONS ……... 10

AUTHORISED USERS ……11

PROVIDING ACCESS TO FIRST LINE CONTROL… 11

ALARMS AND RESTRICTIONS……..12

CAVEATS……12

ADDITIONAL CHECKS……12

PROTOCOLS……...13

DEFINITIONS

1) **TRAVEL DOCUMENT –** identity document used for traveling, recognized by international, regional or bilateral agreements

2) **STOLEN BLANKS-** travel document books that are stolen blank prior to being issued to a bearer

3) **LOST/STOLEN TRAVEL DOCUMENTS** – TD that have been issued to a bearer, but have been lost by or stolen from the bearer

4) **OWNER OF THE DATA** – information on lost/stolen travel documents can be uploaded, shared, updated and deleted **only by the issuing country.**

5) **AUTONOMUS DATABASE- a**n autonomous database means a specialized database not linked to the central database by an indexing system as defined in Article 6.1(b)(3) of the Rules on the Processing of Information for the Purposes of International Police Co-operation (RPI)

6) **BENEFICIARY** – means a National Central Bureau (NCB), national institution, international entity, or authorized by the General Secretariat to access a police information system directly, as defined in Article 20.1(a) of the RPI

7) **DATA SET** – means the mandatory information that in the Stolen Travel Documents System, identifies the travel document
    a. Country of Origin
    b. Passport or Visa
    c. Stolen Blank or Lost/Stolen from Bearer
    d. Document Number

8) **CASE INFORMATION** – Optional information - circumstances surrounding the loss or theft of a travel document

9) **STD SEARCH REQUEST** – search request includes country of origin and document type and number submitted to the Interpol STD database. **Only** document identification number is sufficient to make a query.

PREAMBLE

Considering Article 2 of Interpol's Constitution, which provides that its aims are to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights" and to establish and develop all institutions likely to contribute effectively to the prevention as well as the suppression of ordinary law crimes,

Considering Article 3 of Interpol's Constitution that forbids Interpol from undertaking any intervention or activities of a political, military, religious or racial character,

Deeming that the processing of information constitutes an essential tool for co-operation between all the Interpol Countries, thereby allowing Interpol to fulfill its mission,

Bearing in mind Article 26(c) of Interpol's Constitution, which provides that the General Secretariat shall serve as a technical and information center, and thus be responsible for processing police information,

Also bearing in mind that the processing of information by the General Secretariat (within Interpol's building and premises) is not subject to any national laws,

Considering that under the terms of Article 8(b) and Article 8(d) of Interpol's Constitution, the General Assembly is empowered to determine principles and lay down the general measures suitable for attaining the objectives of Interpol as given in Article 2 of the Interpol Constitution, and to determine any other regulations deemed necessary,

A principle role of Interpol is the efficient and safe transfer between law enforcement agencies of police information appropriate to developments and applications of police investigations and reflected in the second of our core functions.

Law enforcement entities need to be able to identify use of travel related documents to prevent criminals or criminal groups from:

- Crossing international borders,
- Hiding their true identity and
- Performing criminal activities through the use of stolen or falsified travel documents.

For this, the first level of law enforcement control, such as border police or immigration, need to verify the validity of travel documents through a system that allows for accurate and up-to-date data comparison that is available on a real time basis.

Therefore, the General Secretariat has developed the ASF-STD database, which has been operational since June 2002.

PURPOSE AND FUNCTION – DATABASE/SYSTEM

Purpose

Enabling law enforcement entities to impede use of lost/stolen travel documents, used in an illegal manner

Function

The exchange of accurate, reliable, and on a real time basis available information on lost/stolen travel documents, accessible from the collection created in the General Secretariat and/or from national databases, using the Interpol I 24/7 network.

DATA INPUT REQUIREMENTS

ASF-STD is a collection of core travel document related data, requiring the following indexes:

1) The following information from a ***stolen*** travel document must be provided:

    i) **Issuing country (ICAO three letter code)** – reference ICAO Doc 9303, Appendix 2
    ii) **Type of document (code table)** - reference ICAO Doc 9303, Appendix 3
    iii) **Document identity number (DIN**)
    iv) Type of fraud (stolen blank or stolen from bearer)
    v) Country of theft (stolen blank)

2) The following information from a ***lost*** travel document must be provided:

    i) **Issuing country (ICAO three letter code)** - reference ICAO Doc 9303, Appendix 2
    ii) **Type of document (code table)** – reference ICAO Doc 9303, Appendix 3
    iii) Document identity number (DIN)
    iv) Type of fraud (lost from bearer)

Additionally, depending on the choice of the contributing Interpol member country, the system allows for additional non-nominal information concerning the document or the event to be provided.

DATA PROCESSING

DATA TRANSFER

Prescribed data set can be shared, exchanged or made accessible for queries from national systems either through uploading the central collection in the General Secretariat or through data sharing proposals available through Interpol I 24/7 Communication Network.

UPLOADING COLLECTION IN IPSG

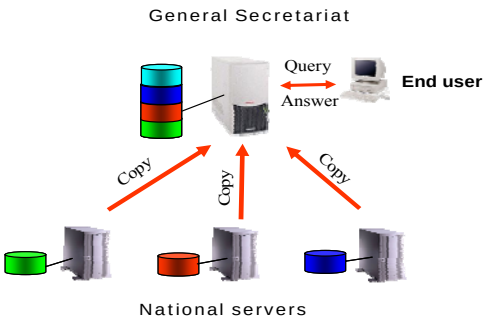
Travel document records, containing the prescribed minimum data set in the form of the acceptable media (e.g. CD), using EDIPOL format (procedure described in details in the existing ASD/STD user manual) or I 24/7 functionalities, can be provided to the member country NCB for uploading the central collection within Interpol Secretariat General (IPSG). This solution is recommended for those member countries not holding a national database or those deciding not to use data sharing solutions.

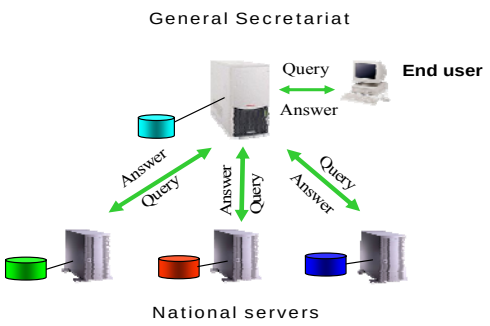
I-24/7 DATA SHARING

For all member countries having their own national systems in place this solution is recommended. Using I 24/7 data sharing functionalities, member countries can keep the collection of their own lost/stolen travel documents prescribed data set, within the country (no copies, no uploads), running their national procedure for updates and maintenance. Following is the general scheme of the recommended model:

BUSINESS-TO-BUSINESS – PRINCIPLES 2

Database sharing with Business-to-Business





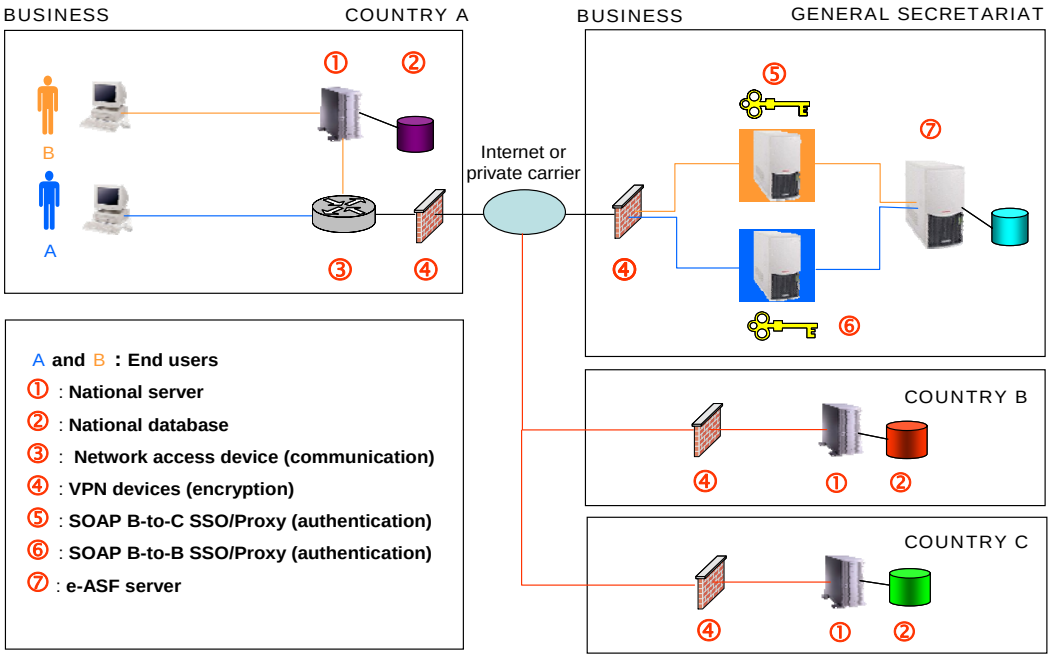
WITHOUT DATA SHARING

- Multiple copies of the same information
- Loss of control of the information
- Loss of quality and integrity of the information
- Huge volume of data at GS

WITH DATA SHARING

- No copies, only publication of information
- Better control at national level
- More control of quality and integrity
- More control of use of the information

BUSINESS-TO-BUSINESS – DATA SHARING



DATA ACCESS

ASF-STD is accessible to every National Central Bureau of Interpol (NCB) for queries and uploading. NCB has a direct link with the central system and lost/stolen travel documents records are available through the I-24/7 Dashboard e-ASF function or Easy Form interface. However, this accessibility is not recommended due to practical and operational reasons: NCB should not be the final user of information available in the system. Information needs to be accessible to the first line control: border police, immigration and authorities checking validity of travel documents.

Therefore the following solution is recommended for the users:

1) ASF-STD has to be used and be accessible for the first law enforcement line of control or immigration control through the following functionalities and quality:

   i) **Real time basis accessibility** – possible simultaneous multimillion queries

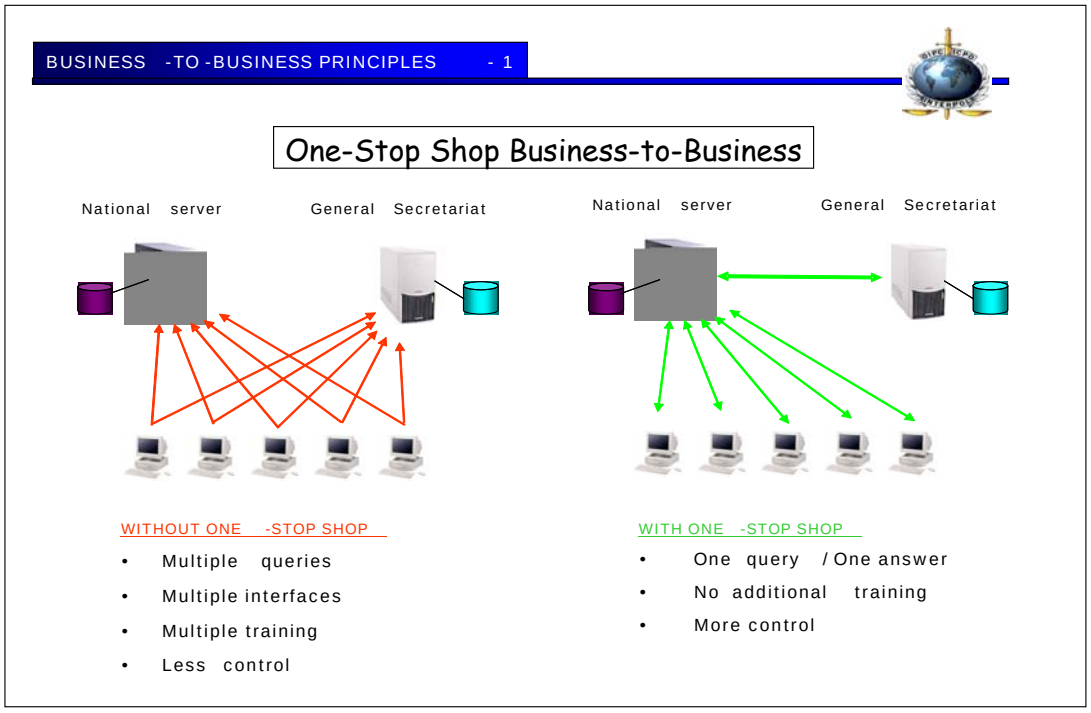
   ii) **Accurate and up to date data**

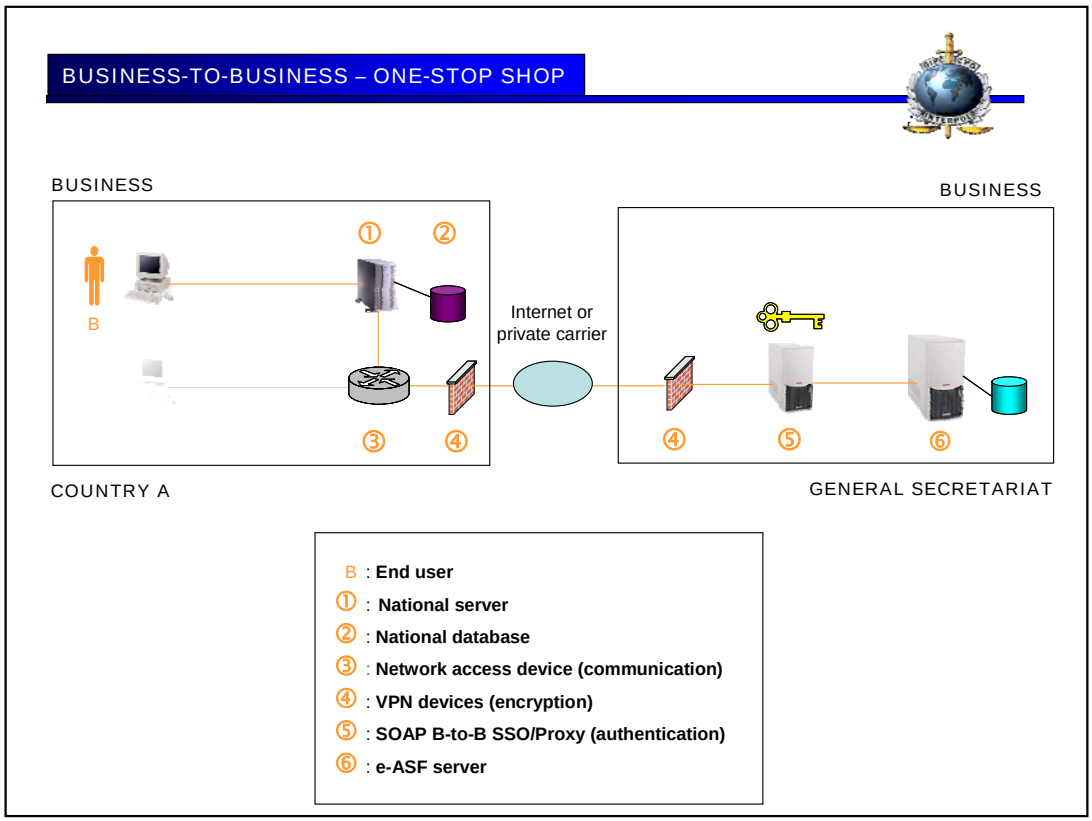
   iii) **Automatic data query, where possible, through the passport's machine readable zone**

   iv) **Issuing country's control over the data (restrictions, alarms, etc...)**

2) I-24/7 Interpol's Global Communication System, with Internet technology, has been developed to enable all the above-mentioned functionalities. Besides an "ordinary" inquiry IPSG database, the system includes possible accessibility of the information from the source itself, such as the exchange of information between national systems in the network.

Recommended solution in the general scheme:





RIGHTS AND OBLIGATIONS

NCB's RIGHTS

In their capacity of national contact point[1] and member country representative, prior authorization to access the database by a national institution that access will have to be granted by the concerned NCB.

In their capacity of source of information, NCBs may impose access restrictions on the information which it records in the database.

OBLIGATIONS OF NCBs AND AUTHORISED USERS

NCBs and authorized entities must ensure, prior to any access authorization that such access is for the purpose of international police co-operation.

NCBs must inform the General Secretariat of new access rights granted to national institutions or any entity concerned with enforcement of the criminal law (reference to the RPI). Such information will permit the entities which have supplied personal information to exercise their right to impose restrictions.

NCBs and authorized entities must take all appropriate measures to ensure that their designated users of the police information system observe the provisions of Interpol Rules on the processing of information for the purposes of international police co-operation (RPI) and the texts to which they refer.

(See proposal for undertakings in appendix) In particular, the NCBs and authorized entities shall:

1. Use all appropriate means to ensure that the persons and entities they authorize are aware of and are able to observe the provisions of the RPI and the texts to which they refer, and that they receive appropriate training for that purpose;
2. Forward the information communicated by the General Secretariat in application of Article 4.4 of the RPI[2], to the persons and entities they authorize;
3. To the extent possible undertake necessary activities to ascertain that the said rules and the texts to which they refer are being respected and communicate the results to the General Secretariat;
4. Inform the General Secretariat of any problem connected with the use of the said system, and/or with the implementation of, or respect for, the applicable rules.

[1] Article 32 Interpol Constitution

[2] Article 4.4 RPI refers to the obligations of the General Secretariat to inform NCBs of new access rights granted authorized entities.

NCBs and authorized entities are responsible for the information they provide. They must ensure that the information they provide is accurate, relevant, and kept updated. Prior to the use of any information, its accuracy and relevancy must be checked.

NCBs and authorized entities must ensure that the information is processed in the context of the laws existing in their countries, in accordance with international convention and Interpol Constitution.

AUTHORISED USERS

Authorized users must observe Interpol rules on processing information (RPI) and the texts to which they refer (see undertakings in appendix).

Authorized users must refrain from having recourse to Interpol to communicate an item of information or to request the retention of an item of information in the Organization's files if that information can no longer be retained in their files by virtue of the applicable local or national laws, in conformity with Article 17.1(g) of the RPI.

Authorized users must ascertain, prior to making any use of an item of information obtained through Interpol channels, that the information concerned is still topical, accurate, and relevant, an that no restrictions have been placed on its retransmission

PROVIDING ACCESS TO FIRST LINE OF CONTROL

NCBs of Interpol are to co-ordinate national level accessibility of information towards the first line users. It is recommended that the I-24/7 National Security Officer, which is to be nominated in every NCB, has to be involved for this task.

ALARMS AND RESTRICTIONS

In the present situation, a positive match in the ASF-STD database will automatically generate an alarm for the concerned NCB in a maximum of 15 minutes.

The new architecture specifications require an instant automatic alarm message be sent to the issuing country's authority. Ideally, the authority, specifically those using I-24/7 on line data sharing, should be available 24 hours per day for data verification.

Interpol Countries maintain the right to restrict access to their data by another country or group of countries. These restrictions can be applied by the Interpol Country while still making their data available to the ASF-STD database authorized users (uploading or data sharing).

CAVEATS

Positive match (aka: hit) message contains the following text in Interpol's four official languages:

*"Before taking any further action, this match **must** be confirmed **through the passport issuing country NCB.** In the event that the issuing **country NCB** is not available, the Command and Coordination Center (CCC) at Interpol General Secretariat **must** be contacted."*

ADDITIONAL CHECKS

When contact has been established with the issuing country NCB or authorized responsible authority for a positive hit confirmation, the following questions from the querying country should be answered:

i) Name and date of birth
ii) Mother's maiden name
iii) Mother's date of birth
iv) Father's date of birth

BEST PRACTICE IN CASE OF A POSITIVE HIT CONFIRMATION

In case of a confirmation of the positive hit from the issuing country, the legal procedure of the querying country should be followed. After the closure of the criminal/administrative case and if the procedure foresees the seizure of the travel document, the seized document should be returned to the nearest diplomatic representation of the issuing country.

Appendix 1

LETTER OF COMMITMENT

I the undersigned _____(forename and family name) _____ (title of post in the authorized entity concerned), empowered to represent the (name of entity) :

undertake to comply with Interpol's Rules on the Processing of Information for international police co-operation (Appendix 1);
undertake to comply with the I-24/7 Security Charter (Appendix 2);
undertake to ensure that any user habilitated to access the [name of database]////// Database complies with the above;
recognize that in case of a failure to comply with these rules, all services provided by the Organization are Interpol's property and may be suspended without prior notice;

Done at ..... on .....
Signature: .....
Family name, forename, position: .....

Signed in ……. on _____/_____/_____.
Signature of the user,

Surname, first name:
……..……....
Role :
……..……
…

Undertaking on-line

Text to be inserted for acceptance on-line by any new authorized entity and <u>its users</u> prior to validation of first connection to Interpol's police information system:

"I declare having acknowledged and accepted <u>the general conditions of use of Interpol police information system"</u>

<u>The general conditions of use of Interpol police information system:</u>

Windows to be opened: 1. Rules on processing of information for international police co-operation (RPI)

2. Security Charter

(additional windows shall be added whenever new rules are adopted, for example implementing rules on the RPI)

☐

If the user did not tick the corresponding box, the validation of the first connection to Interpol police information system can not be continued. The following text should appear on the screen:

"To take into account your request for access, you should acknowledge and accept the general conditions of use of Interpol police information system."

APPENDIX 2

Codes for designation of nationality, place of birth or issuing State/authority (for the purposes of MRTD in accordance with ICAO Doc 9303)

Numeric	Alpha-3	Alpha-2	Local ISO codes	Country / Region
004	AFG	AF	(ISO 3166-2)	Afghanistan
248	ALA	AX	(ISO 3166-2)	Ŭand Islands
008	ALB	AL	(ISO 3166-2)	Albania
012	DZA	DZ	(ISO 3166-2)	Algeria
016	ASM	AS	(ISO 3166-2)	American Samoa
020	AND	AD	(ISO 3166-2)	Andorra
024	AGO	AO	(ISO 3166-2)	Angola
660	AIA	AI	(ISO 3166-2)	Anguilla
010	ATA	AQ	(ISO 3166-2)	Antarctica
028	ATG	AG	(ISO 3166-2)	Antigua and Barbuda
032	ARG	AR	(ISO 3166-2)	Argentina
051	ARM	AM	(ISO 3166-2)	Armenia
533	ABW	AW	(ISO 3166-2)	Aruba
036	AUS	AU	(ISO 3166-2)	Australia
040	AUT	AT	(ISO 3166-2)	Austria
031	AZE	AZ	(ISO 3166-2)	Azerbaijan
044	BHS	BS	(ISO 3166-2)	Bahamas
048	BHR	BH	(ISO 3166-2)	Bahrain
050	BGD	BD	(ISO 3166-2)	Bangladesh
052	BRB	BB	(ISO 3166-2)	Barbados
112	BLR	BY	(ISO 3166-2)	Belarus
056	BEL	BE	(ISO 3166-2)	Belgium
084	BLZ	BZ	(ISO 3166-2)	Belize
204	BEN	BJ	(ISO 3166-2)	Benin
060	BMU	BM	(ISO 3166-2)	Bermuda
064	BTN	BT	(ISO 3166-2)	Bhutan
068	BOL	BO	(ISO 3166-2)	Bolivia
070	BIH	BA	(ISO 3166-2)	Bosnia and Herzegovina
072	BWA	BW	(ISO 3166-2)	Botswana
074	BVT	BV	(ISO 3166-2)	Bouvet Island
076	BRA	BR	(ISO 3166-2)	Brazil
086	IOT	IO	(ISO 3166-2)	British Indian Ocean Territory
096	BRN	BN	(ISO 3166-2)	Brunei Darussalam
100	BGR	BG	(ISO 3166-2)	Bulgaria
854	BFA	BF	(ISO 3166-2)	Burkina Faso
108	BDI	BI	(ISO 3166-2)	Burundi
116	KHM	KH	(ISO 3166-2)	Cambodia
120	CMR	CM	(ISO 3166-2)	Cameroon
124	CAN	CA	(ISO 3166-2)	Canada
132	CPV	CV	(ISO 3166-2)	Cape Verde
136	CYM	KY	(ISO 3166-2)	Cayman Islands
140	CAF	CF	(ISO 3166-2)	Central African Republic
148	TCD	TD	(ISO 3166-2)	Chad
152	CHL	CL	(ISO 3166-2)	Chile
156	CHN	CN	(ISO 3166-2)	China

162	CXR	CX	(ISO 3166-2)	Christmas Island
166	CCK	CC	(ISO 3166-2)	Cocos (Keeling) Islands
170	COL	CO	(ISO 3166-2)	Colombia
174	COM	KM	(ISO 3166-2)	Comoros
178	COG	CG	(ISO 3166-2)	Congo, Republic of the
180	COD	CD	(ISO 3166-2)	Congo, The Democratic Republic Of The
184	COK	CK	(ISO 3166-2)	Cook Islands
188	CRI	CR	(ISO 3166-2)	Costa Rica
384	CIV	CI	(ISO 3166-2)	C?d'Ivoire
191	HRV	HR	(ISO 3166-2)	Croatia
192	CUB	CU	(ISO 3166-2)	Cuba
196	CYP	CY	(ISO 3166-2)	Cyprus
203	CZE	CZ	(ISO 3166-2)	Czech Republic
208	DNK	DK	(ISO 3166-2)	Denmark
262	DJI	DJ	(ISO 3166-2)	Djibouti
212	DMA	DM	(ISO 3166-2)	Dominica
214	DOM	DO	(ISO 3166-2)	Dominican Republic
218	ECU	EC	(ISO 3166-2)	Ecuador
818	EGY	EG	(ISO 3166-2)	Egypt
222	SLV	SV	(ISO 3166-2)	El Salvador
226	GNQ	GQ	(ISO 3166-2)	Equatorial Guinea
232	ERI	ER	(ISO 3166-2)	Eritrea
233	EST	EE	(ISO 3166-2)	Estonia
231	ETH	ET	(ISO 3166-2)	Ethiopia
???	???	EU	(ISO 3166-2)	European Union
238	FLK	FK	(ISO 3166-2)	Falkland Islands (Malvinas)*
234	FRO	FO	(ISO 3166-2)	Faroe Islands
242	FJI	FJ	(ISO 3166-2)	Fiji
246	FIN	FI	(ISO 3166-2)	Finland
250	FRA	FR	(ISO 3166-2)	France
254	GUF	GF	(ISO 3166-2)	French Guiana
258	PYF	PF	(ISO 3166-2)	French Polynesia
260	ATF	TF	(ISO 3166-2)	French Southern Territories
266	GAB	GA	(ISO 3166-2)	Gabon
270	GMB	GM	(ISO 3166-2)	Gambia
268	GEO	GE	(ISO 3166-2)	Georgia
276	DEU	DE	(ISO 3166-2)	Germany
288	GHA	GH	(ISO 3166-2)	Ghana
292	GIB	GI	(ISO 3166-2)	Gibraltar
300	GRC	GR	(ISO 3166-2)	Greece
304	GRL	GL	(ISO 3166-2)	Greenland
308	GRD	GD	(ISO 3166-2)	Grenada
312	GLP	GP	(ISO 3166-2)	Guadeloupe
316	GUM	GU	(ISO 3166-2)	Guam
320	GTM	GT	(ISO 3166-2)	Guatemala
324	GIN	GN	(ISO 3166-2)	Guinea
624	GNB	GW	(ISO 3166-2)	Guinea-Bissau
328	GUY	GY	(ISO 3166-2)	Guyana
332	HTI	HT	(ISO 3166-2)	Haiti
334	HMD	HM	(ISO 3166-2)	Heard Island and McDonald Islands

340	HND	HN	(ISO 3166-2)	Honduras
344	HKG	HK	(ISO 3166-2)	Hong Kong Special Administrative Region of China
348	HUN	HU	(ISO 3166-2)	Hungary
352	ISL	IS	(ISO 3166-2)	Iceland
356	IND	IN	(ISO 3166-2)	India
360	IDN	ID	(ISO 3166-2)	Indonesia
364	IRN	IR	(ISO 3166-2)	Iran, Islamic Republic of
368	IRQ	IQ	(ISO 3166-2)	Iraq
372	IRL	IE	(ISO 3166-2)	Ireland
376	ISR	IL	(ISO 3166-2)	Israel
380	ITA	IT	(ISO 3166-2)	Italy
388	JAM	JM	(ISO 3166-2)	Jamaica
392	JPN	JP	(ISO 3166-2)	Japan
400	JOR	JO	(ISO 3166-2)	Jordan
398	KAZ	KZ	(ISO 3166-2)	Kazakhstan
404	KEN	KE	(ISO 3166-2)	Kenya
296	KIR	KI	(ISO 3166-2)	Kiribati
408	PRK	KP	(ISO 3166-2)	Korea, Democratic People's Republic of
410	KOR	KR	(ISO 3166-2)	Korea, Republic of
414	KWT	KW	(ISO 3166-2)	Kuwait
417	KGZ	KG	(ISO 3166-2)	Kyrgyzstan
418	LAO	LA	(ISO 3166-2)	Lao People's Democratic Republic
428	LVA	LV	(ISO 3166-2)	Latvia
422	LBN	LB	(ISO 3166-2)	Lebanon
426	LSO	LS	(ISO 3166-2)	Lesotho
430	LBR	LR	(ISO 3166-2)	Liberia
434	LBY	LY	(ISO 3166-2)	Libyan Arab Jamahiriya
438	LIE	LI	(ISO 3166-2)	Liechtenstein
440	LTU	LT	(ISO 3166-2)	Lithuania
442	LUX	LU	(ISO 3166-2)	Luxembourg
446	MAC	MO	(ISO 3166-2)	Macao Special Administrative Region of China
807	MKD	MK	(ISO 3166-2)	The Former Yugoslav Republic of Macedonia
450	MDG	MG	(ISO 3166-2)	Madagascar
454	MWI	MW	(ISO 3166-2)	Malawi
458	MYS	MY	(ISO 3166-2)	Malaysia
462	MDV	MV	(ISO 3166-2)	Maldives
466	MLI	ML	(ISO 3166-2)	Mali
470	MLT	MT	(ISO 3166-2)	Malta
584	MHL	MH	(ISO 3166-2)	Marshall Islands
474	MTQ	MQ	(ISO 3166-2)	Martinique
478	MRT	MR	(ISO 3166-2)	Mauritania
480	MUS	MU	(ISO 3166-2)	Mauritius
175	MYT	YT	(ISO 3166-2)	Mayotte
484	MEX	MX	(ISO 3166-2)	Mexico
583	FSM	FM	(ISO 3166-2)	Micronesia, Federated States of
498	MDA	MD	(ISO 3166-2)	Moldova, Republic of
492	MCO	MC	(ISO 3166-2)	Monaco
496	MNG	MN	(ISO 3166-2)	Mongolia
500	MSR	MS	(ISO 3166-2)	Montserrat
504	MAR	MA	(ISO 3166-2)	Morocco

508	MOZ	MZ	(ISO 3166-2)	Mozambique
104	MMR	MM	(ISO 3166-2)	Myanmar
516	NAM	NA	(ISO 3166-2)	Namibia
520	NRU	NR	(ISO 3166-2)	Nauru
524	NPL	NP	(ISO 3166-2)	Nepal
528	NLD	NL	(ISO 3166-2)	Netherlands
530	ANT	AN	(ISO 3166-2)	Netherlands Antilles
540	NCL	NC	(ISO 3166-2)	New Caledonia
554	NZL	NZ	(ISO 3166-2)	New Zealand
558	NIC	NI	(ISO 3166-2)	Nicaragua
562	NER	NE	(ISO 3166-2)	Niger
566	NGA	NG	(ISO 3166-2)	Nigeria
570	NIU	NU	(ISO 3166-2)	Niue
574	NFK	NF	(ISO 3166-2)	Norfolk Island
580	MNP	MP	(ISO 3166-2)	Northern Mariana Islands
578	NOR	NO	(ISO 3166-2)	Norway
512	OMN	OM	(ISO 3166-2)	Oman
586	PAK	PK	(ISO 3166-2)	Pakistan
585	PLW	PW	(ISO 3166-2)	Palau
275	PSE	PS	(ISO 3166-2)	Palestinian Territory, Occupied
591	PAN	PA	(ISO 3166-2)	Panama
598	PNG	PG	(ISO 3166-2)	Papua New Guinea
600	PRY	PY	(ISO 3166-2)	Paraguay
604	PER	PE	(ISO 3166-2)	Peru
608	PHL	PH	(ISO 3166-2)	Philippines
612	PCN	PN	(ISO 3166-2)	Pitcairn
616	POL	PL	(ISO 3166-2)	Poland
620	PRT	PT	(ISO 3166-2)	Portugal
630	PRI	PR	(ISO 3166-2)	Puerto Rico
634	QAT	QA	(ISO 3166-2)	Qatar
638	REU	RE	(ISO 3166-2)	R鴿ion
642	ROU	RO	(ISO 3166-2)	Romania
643	RUS	RU	(ISO 3166-2)	Russian Federation
646	RWA	RW	(ISO 3166-2)	Rwanda
654	SHN	SH	(ISO 3166-2)	Saint Helena
659	KNA	KN	(ISO 3166-2)	Saint Kitts and Nevis
662	LCA	LC	(ISO 3166-2)	Saint Lucia
666	SPM	PM	(ISO 3166-2)	Saint-Pierre and Miquelon
670	VCT	VC	(ISO 3166-2)	Saint Vincent and the Grenadines
882	WSM	WS	(ISO 3166-2)	Samoa
674	SMR	SM	(ISO 3166-2)	San Marino
678	STP	ST	(ISO 3166-2)	S Tom颠nd Pr ipe
682	SAU	SA	(ISO 3166-2)	Saudi Arabia
686	SEN	SN	(ISO 3166-2)	Senegal
891	SCG	CS	(ISO 3166-2)	Serbia and Montenegro
690	SYC	SC	(ISO 3166-2)	Seychelles
694	SLE	SL	(ISO 3166-2)	Sierra Leone
702	SGP	SG	(ISO 3166-2)	Singapore
703	SVK	SK	(ISO 3166-2)	Slovakia
705	SVN	SI	(ISO 3166-2)	Slovenia

090	SLB	SB	(ISO 3166-2)	Solomon Islands
706	SOM	SO	(ISO 3166-2)	Somalia
710	ZAF	ZA	(ISO 3166-2)	South Africa
239	SGS	GS	(ISO 3166-2)	South Georgia and the South Sandwich Islands
724	ESP	ES	(ISO 3166-2)	Spain
144	LKA	LK	(ISO 3166-2)	Sri Lanka
736	SDN	SD	(ISO 3166-2)	Sudan
740	SUR	SR	(ISO 3166-2)	Suriname
744	SJM	SJ	(ISO 3166-2)	Svalbard and Jan Mayen
748	SWZ	SZ	(ISO 3166-2)	Swaziland
752	SWE	SE	(ISO 3166-2)	Sweden
756	CHE	CH	(ISO 3166-2)	Switzerland
760	SYR	SY	(ISO 3166-2)	Syrian Arab Republic
158	TWN	TW	(ISO 3166-2)	Taiwan, Province of China
762	TJK	TJ	(ISO 3166-2)	Tajikistan
834	TZA	TZ	(ISO 3166-2)	Tanzania, United Republic Of
764	THA	TH	(ISO 3166-2)	Thailand
626	TLS	TL	(ISO 3166-2)	Timor-Leste
768	TGO	TG	(ISO 3166-2)	Togo
772	TKL	TK	(ISO 3166-2)	Tokelau
776	TON	TO	(ISO 3166-2)	Tonga
780	TTO	TT	(ISO 3166-2)	Trinidad and Tobago
788	TUN	TN	(ISO 3166-2)	Tunisia
792	TUR	TR	(ISO 3166-2)	Turkey
795	TKM	TM	(ISO 3166-2)	Turkmenistan
796	TCA	TC	(ISO 3166-2)	Turks and Caicos Islands
798	TUV	TV	(ISO 3166-2)	Tuvalu
800	UGA	UG	(ISO 3166-2)	Uganda
804	UKR	UA	(ISO 3166-2)	Ukraine
784	ARE	AE	(ISO 3166-2)	United Arab Emirates
826	GBR	GB	(ISO 3166-2)	United Kingdom
840	USA	US	(ISO 3166-2)	United States
581	UMI	UM	(ISO 3166-2)	United States Minor Outlying Islands
858	URY	UY	(ISO 3166-2)	Uruguay
860	UZB	UZ	(ISO 3166-2)	Uzbekistan
548	VUT	VU	(ISO 3166-2)	Vanuatu
336	VAT	VA	(ISO 3166-2)	Vatican City State
862	VEN	VE	(ISO 3166-2)	Venezuela
704	VNM	VN	(ISO 3166-2)	Viet Nam
092	VGB	VG	(ISO 3166-2)	Virgin Islands, British
850	VIR	VI	(ISO 3166-2)	Virgin Islands, U.S.
876	WLF	WF	(ISO 3166-2)	Wallis and Futuna
732	ESH	EH	(ISO 3166-2)	Western Sahara
887	YEM	YE	(ISO 3166-2)	Yemen
894	ZMB	ZM	(ISO 3166-2)	Zambia
716	ZWE	ZW	(ISO 3166-2)	Zimbabwe

Reference

Information on reserved codes taken from "Reserved code elements under ISO 3166-1" published by Secretariat of ISO/TC 46, ISO 3166 Maintenance Agency, 2001-02-13, available on request from ISO 3166 MA.

*A dispute exists between the Governments of Argentina and the United Kingdom of Great Britain and Northern Ireland concerning sovereignty over the Falkland Islands (Malvinas).