ICAO MRTD REPORT
VOLUME 3, NUMBER 3, 2008

Editorial
Managing Editor: Mauricio Siciliano
MRTD Programme—Aviation Security
and Facilitation Policy Section
Tel: +1 (514) 954-8219 ext. 7068
E-mail : msiciliano@icao.int

Anthony Philbin Communications
Senior Editor: Anthony Philbin
Tel: +01 (514) 886-7746
E-mail: info@philbin.ca
Web Site: www.philbin.ca

Production and Design
Bang Marketing
Stéphanie Kennan
Tel: +01 (514) 849-2264
E-mail: info@bang-marketing.com
Web Site: www.bang-marketing.com

Advertising
FCM Communications Inc.
Yves Allard
Tel: +01 (450) 677-3535
Fax: +01 (450) 677-4445
E-mail: fcmcommunications@videotron.ca

Submissions
The *MRTD Report* encourages submissions from interested individuals, organizations and States wishing to share updates, perspectives or analysis related to global civil aviation. For further information on submission deadlines and planned issue topics for future editions of the *MRTD Report*, please contact Mauricio Siciliano, managing editor at: msiciliano@icao.int

Opinions expressed in signed articles or in advertisements appearing in the ICAO *MRTD Report* represent the author's or advertiser's opinion and do not necessarily reflect the views of ICAO. The mention of specific companies or products in articles or advertisements does not imply that they are endorsed or recommended by ICAO in preference to others of a similar nature which are not mentioned or advertised.

The publishers extend their thanks to the companies, organizations and photographers who graciously supplied photographs for this issue.

Published by
International Civil Aviation Organization (ICAO)
999 University Street
Montréal, Québec
Canada H3C 5H7

The objective of the ICAO *MRTD Report* is to provide a comprehensive account of new developments, trends, innovations and applications in the field of MRTDs to the Contracting States of ICAO and the international aeronautical and security communities.

PRINTED BY ICAO

Contents

Identity fraud and digital capability

Identity fraud is a worldwide problem, with criminals and terrorists currently traveling between States using non existent, fabricated identities or identities that have been stolen from a legitimate citizen. Government and law enforcement personnel tend to this problem through a wide range of measures—including improvements in the security of the travel document itself—but Clemens Willemsen of the Dutch Department of Justice argues that in the digital age we may wish to begin considering eliminating ID documents altogether.

Though some of the solutions being presented in the following article may appear straightforward, they also require that those of us involved in the areas of passport issuance and border control may need to change our way of thinking about the very nature of identity documents. The three basic steps that I propose are required for States to diminish identity fraud are:

1. Using identity documents published by official authorities only.
2. Distinguishing between establishing identification with a document and granting rights to the owner of a document.
3. Replacing the physical document by a virtual document.

1. Using identity documents published by official authorities only

Identity documents can be categorized as:

- Primary *(published by an official authority).*
- Secondary *(published by a public or private organization such as a hospital, public transportation service, company, etc).*

A Primary ID document (PID) is handed over by an official authority, such as a State passport office or a regional license bureau branch, after a thorough check on a citizen's administrative and/or biometric identity—making use of, for example, a birth certificate or an expired passport. There are strict procedures surrounding identity establishment and document issuance that are employed by PID sources *(editor's note: see the 'Issuance and Identity' section in MRTD Report Issue 01 2008 for more on this topic).*

A Secondary ID document (SID) is based upon the PID. A hospital for example will admit you as a patient and requires you to show a PID. After verifying it is you, you will be registered and handed a hospital card to serve as a SID. This card identifies you only for hospital purposes and grants you certain rights to specific hospital procedures. This type of SID document is generally significantly less secure than a PID and therefore easier to copy or forge.

It is more recommendable then to use the PID for each visit to organizations that currently distribute SIDs for their own use. In the past, this might have been a problem, but in more and more countries citizens are required now both to carry and to show their PID for official purposes. Therefore they are much more likely today to have it with them at all times.

Under this type of regulated PID environment States and other organizations or more localized government entities would no longer need to concern themselves with the infrastructure, staffing and costs inherent in their SID programmes. Overall citizen privacy would furthermore be augmented by the fact that there would be fewer cards in circulation containing private information that could possibly be lost or stolen.

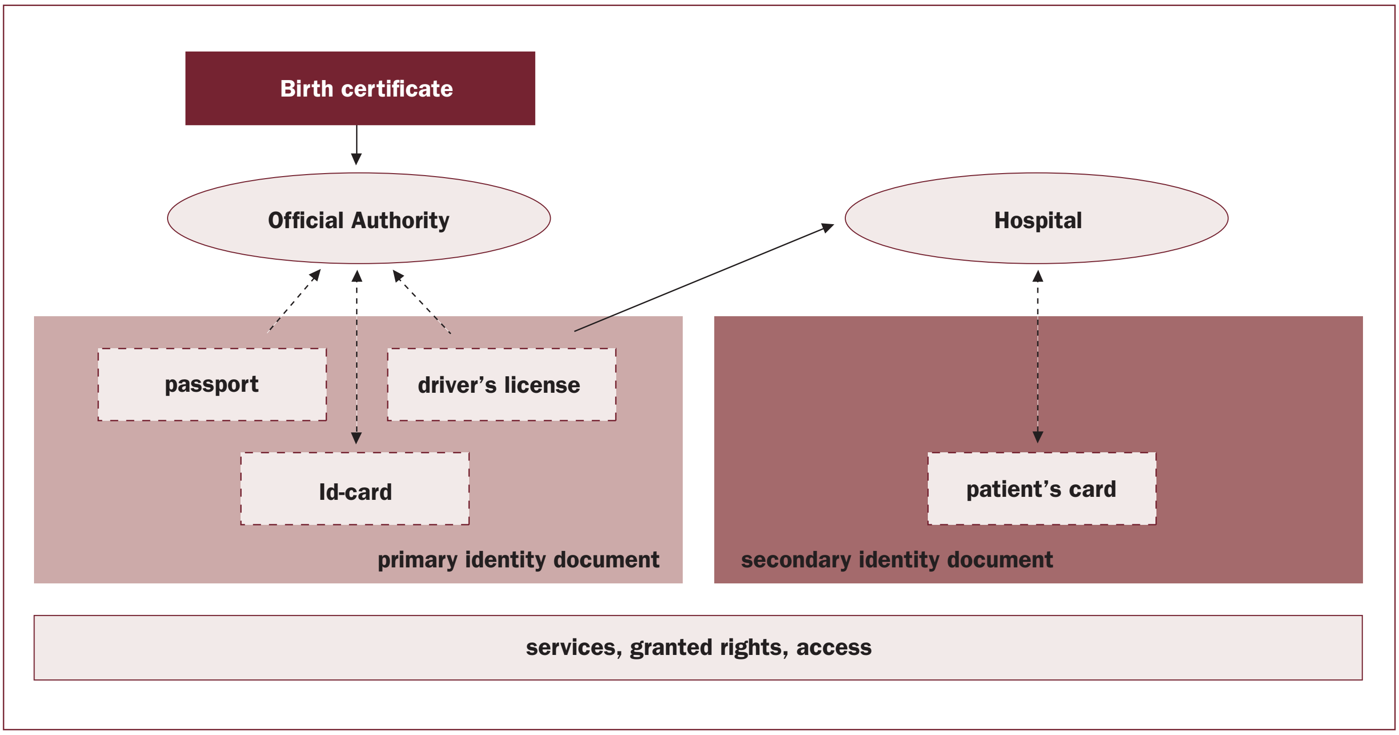
2. Distinguishing between establishing identification with a document and granting rights to the owner of a document

Traditionally, PIDs not only identify the bearer and authenticate him or her for national or international authorities, but also grants certain rights to the bearer, such as:

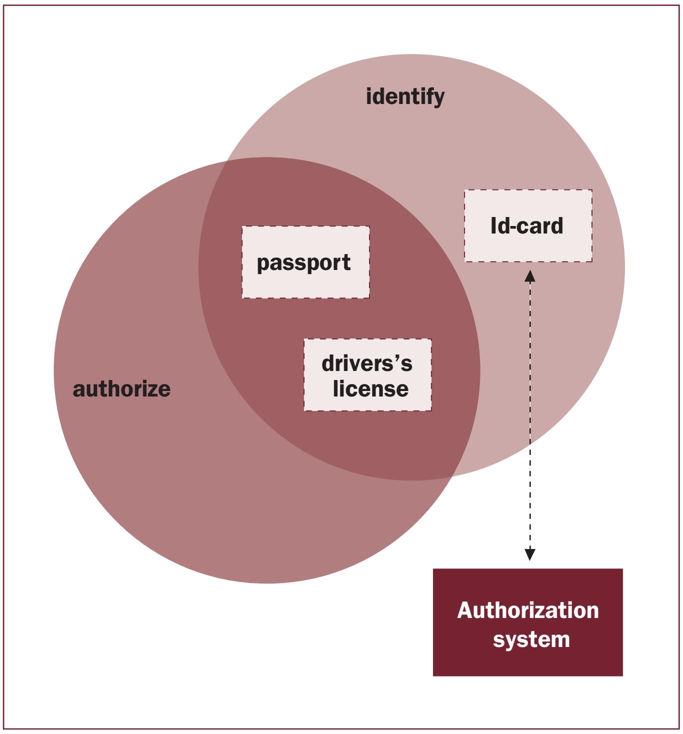
1. *Passport*—identifies and grants the bearer the right to cross certain borders.
2. *Driver's license*—identifies and grants the bearer the right to drive a motor vehicle.
3. *Social security card*—identifies and grants the bearer the right to use social services.

In other words, identity establishment and user rights are combined in the current PIDs. Many SIDs operate in the same fashion:

1. *Library card*—identifies and grants the bearer the right to borrow books.
2. *Credit card*—identifies and grants the bearer the right to spend money.



This combining of ID establishment with bearer rights and permissions was required in the past when physical ID tools and systems (cards and/or other documents) were distinct and separate from the administrative systems that tracked and recorded the bearer's associated permissions. It obviously wasn't practical using paper-based systems to re-verify the bearer's rights at each presenting of their ID and so the ID itself needed to clearly indicate what rights the bearer was entitled to and when these could be exercised, but when viewed in light of current digital capabilities this requirement is no longer necessary.



When all State infrastructures become more developed in this regard it would be advantageous to move away from the current requirements (even with the newer ePassports bearer rights are still reflected on the ID itself as per the needs of older administrative structures) and instead simply use the PID to enable border and customs officials to access real-time indications of the bearer's completely up-to-date rights and permissions.

The advantages of separating identity establishment from rights establishment with PIDs are numerous therefore:

1. Your specific identity card can be stolen but not your granted rights.
2. Granted rights can be checked online and are no longer restrained to the time of issue and the expiration date of the card. It is always up to date.
3. A bearer would only require one PID.
4. There would no longer be a need for SIDs that are less secure then PIDs.
5. When stolen, you only need to report/reapply for one card instead of numerous cards.
6. The real-time and continuous verification of bearer rights would facilitate the identification and removal from circulation of stolen or fraudulent PIDs

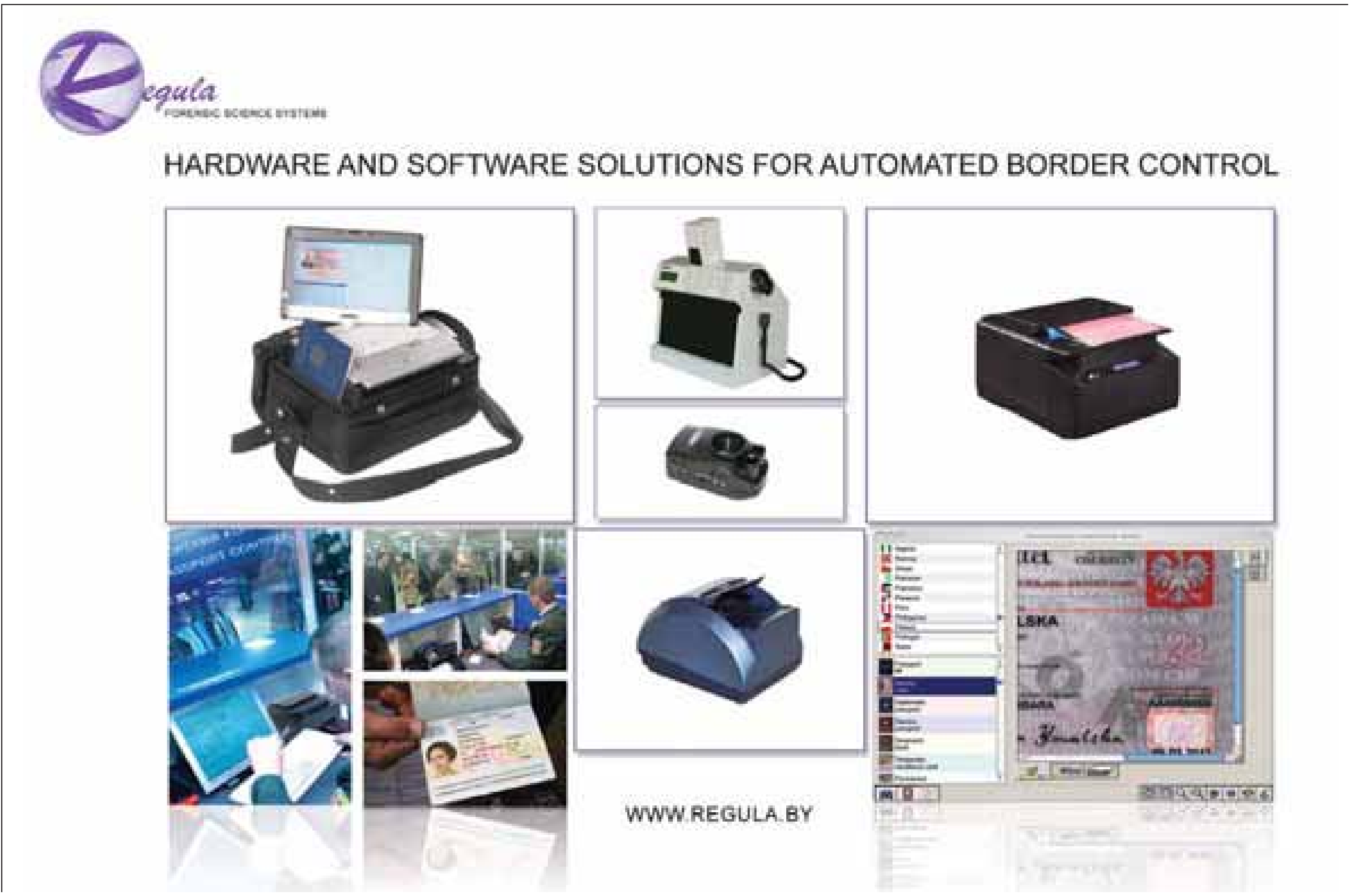
One of the few disadvantages would be that digital systems would need to be available and accessible to officials at all times. System down-time could result in significant impacts to travel and other activities that will always require PID verification. These disadvantages could be dealt with, however, through established procedures now in place to create independent power back ups, information redundancy and mirrored access for essential digital networks—such as those that currently exist in defense and banking systems or other properly secured corporate networks.

An additional hesitancy could also be envisaged by those who might be reluctant to have all their ID establishment reflected in just a single card (especially for suppliers who currently furnish the global population with multiple PIDs and SIDs). For the bearer, however, the separation of rights from ID establishment would minimize the implications of a lost or stolen PID, which brings to mind how a bearer's ID could be established if they were no longer in possession of their only form of physical ID, and where this line of thought would take us if carried to its logical conclusion.

3. Replacing the physical document by a virtual document

The ultimate step in this process would be to eliminate the physical document altogether and replace it with a 'virtual document' (basically the rights information alone that would be displayed electronically when an official queried an individual's rights). Biometric information is currently being employed in the newest ePassports and visas to assist officials in establishing a PID bearer's identity, but why not simply have the traveler submit to biometric scans at point of entry and forego the need for a physical document completely? This would be the next step in the evolution of our ability to ascertain the identification and rights of all citizens in a fully digital age.

Clemens Willemsen works for the Dutch Department of Justice where he is involved in identity management and biometrics. This article is his personal view only and does not necessarily reflect the point of view of his government or its respective departments. ■


Regula
FORENSIC SCIENCE SYSTEMS
HARDWARE AND SOFTWARE SOLUTIONS FOR AUTOMATED BORDER CONTROL
WWW.REGULA.BY