Using 2D Barcodes to Enhance the Security of Machine-Readable Travel Documents (MRTDs)

Version 1.2

Introduction

In today's world the need for document authentication is very real. Control authorities need to be able to verify that a document has not been altered or forged, and that the bearer of the document is the rightful holder of that document. Barcodes, with their extended data capacity, can incorporate sophisticated security features that provide an effective means of document authentication at a checkpoint.

There are dozens of types of one-dimensional (1D) barcodes, with uses ranging from retail point of sale to inventory control. A typical 1D barcode can hold approximately 30 bytes of data – often enough only to provide a reference to a piece of data versus to contain the data. In the context of passports, visas, and ID cards, the amount of space available on a 1D barcode is not sufficient to provide the enhanced security and document authentication features required by many document issuers.

To address this need for enhanced security, ICAO, the International Civil Aviation Organisation, is currently considering a standard for the application of a two-dimensional (2D) barcode on the data page of an MRTD[1]. As proposed, the 2D barcode would be able to accommodate up to 830 bytes, which is sufficient space to include data meaningful for document authentication purposes.

At an inspection point such as an airport, land or sea crossing, a 2D barcode on an MRTD is decoded via an automated document reader. The displayed data can then be compared with:

- the data visible on the document,
- the traveller him/herself (in the case of a facial image),
- a cryptographic digital signature (generated with the Public Key Infrastructure (PKI) of the issuing agency), or
- the original data held in the document issuance database.

By ensuring that the data encoded in the barcode matches any or all of the above, a control authority can be reasonably sure that the document presented is authentic.

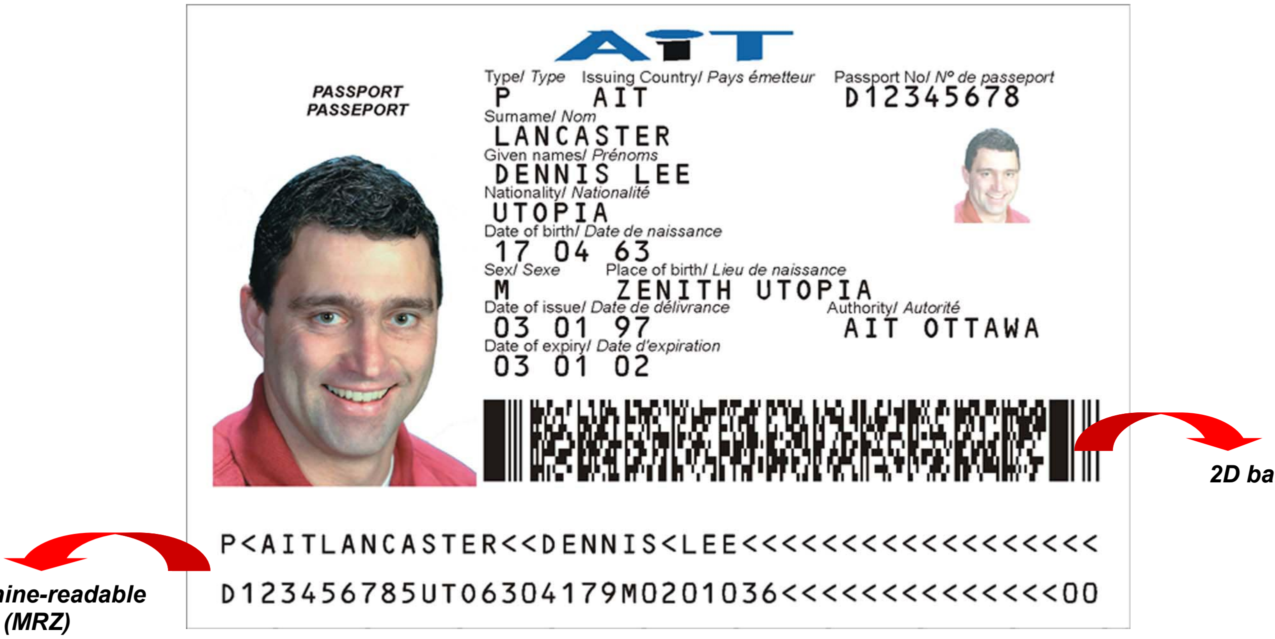
This paper will discuss design and implementation issues surrounding the use of 2D barcodes to enhance the security of an MRTD, and will present recommendations, based on AiT's research, testing and experience.

[1] Throughout this paper, the term MRTD will refer to machine-readable passports, visas and other official travel and identity documents, as outlined in ICAO Doc 9303. At its most recent meeting (June 2000), the Working Group on New Technologies of the ICAO Technical Advisory Group (TAG-MRTD) submitted a comprehensive revision of the specifications for MRTDs, which is expected to become part of Doc 9303, Fifth Edition.

PDF417: A Layman's Overview of the Specification

There are many different 2D barcode symbologies available; most of which are proprietary. One that appears to be gaining international acceptance is the PDF417 specification[2], written by Symbol Technologies and published by AIM, Inc. ICAO is considering a standard for the inclusion of a 2D barcode on the data page of an MRTD, and ICAO Doc 9303 currently lists PDF417 as the only item on the accepted list of symbologies. Other vendors, however, are opening up their previously proprietary standards and are positioning themselves to be included on the ICAO-accepted list of symbologies. For the purposes of this discussion, it will be assumed that 2D barcodes, whenever referred to, are 2D barcodes according to the PDF417 specification.

Figure 1 illustrates the placement of a 2D barcode on an ICAO-compliant passport.



PASSPORT
PASSEPORT

Type/ *Type*: P
Issuing Country/ *Pays émetteur*: AIT
Passport No/ *Nº de passeport*: D12345678
Surname/ *Nom*: LANCASTER
Given names/ *Prénoms*: DENNIS LEE
Nationality/ *Nationalité*: UTOPIA
Date of birth/ *Date de naissance*: 17 04 63
Sex/ *Sexe*: M
Place of birth/ *Lieu de naissance*: ZENITH UTOPIA
Date of issue/ *Date de délivrance*: 03 01 97
Authority/ *Autorité*: AIT OTTAWA
Date of expiry/ *Date d'expiration*: 03 01 02

P<AITLANCASTER<<DENNIS<LEE<<<<<<<<<<<<<<<<<<
D123456785UT06304179M0201036<<<<<<<<<<<<<<00

2D barcode

machine-readable zone (MRZ)

Figure 1 – Passport with PDF417 2D barcode

A 2D barcode is comprised of hundreds of smaller elements, called features or modules, which represent data. There is a direct relationship between the amount of data held in the barcode and the readability of the data. As the individual feature size shrinks, more data can be put on the barcode, but the readability of that data is reduced.

[2] For descriptions of the character encoding, symbol structure, reference decode algorithm, and symbol quality measurements for PDF417, please refer to AIM, Inc., "Uniform Symbology Specification – PDF417", September 1994.

The ICAO MRTD recommendation calls for a 2D barcode that is 80 mm wide and 18 mm high, with a minimum feature size of 0.17 mm and a 3:1 aspect ratio. A PDF417 barcode can contain up to 830 bytes, with an error correction level of 5.

Error correction is a method of enhancing readability by including redundant data that can be called upon if the original data in a barcode is not readable. The specification allows for the error correction level to be user configurable; however, as the level of error correction increases, there are fewer remaining bytes available for data in the barcode. To optimize the readability of a 2D barcode in an MRTD, AiT recommends the error correction level be set at 5 and that there be sufficient white space around the symbol.

Figures 2 through 5 below illustrate 2D barcodes with varying feature sizes, along with the corresponding decoded image contained in the barcode (compressed using AiT's FiCA algorithm). As the number of bytes of data increases there is a noticeable difference in the size of the features within each barcode. The original photo size was 30 kilobytes.

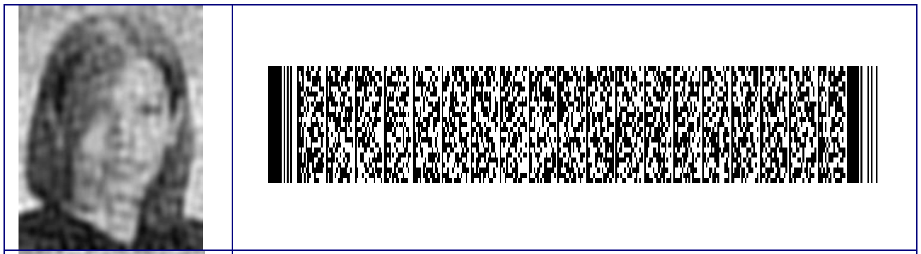


Figure 2 – barcode contains 250 bytes of image data

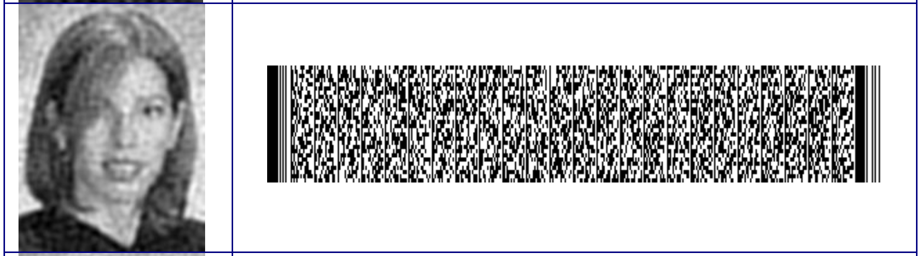


Figure 3 – barcode contains 500 bytes of image data

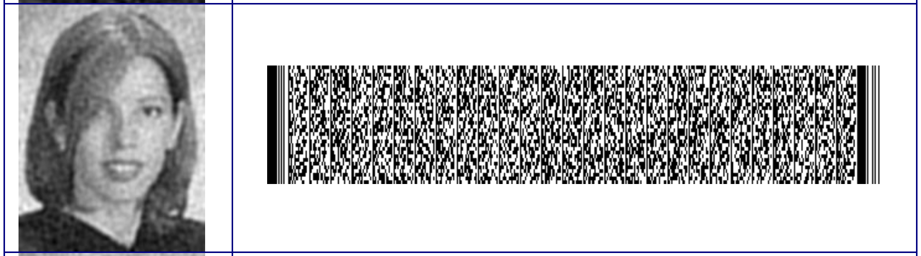


Figure 4 – barcode contains 750 bytes of image data

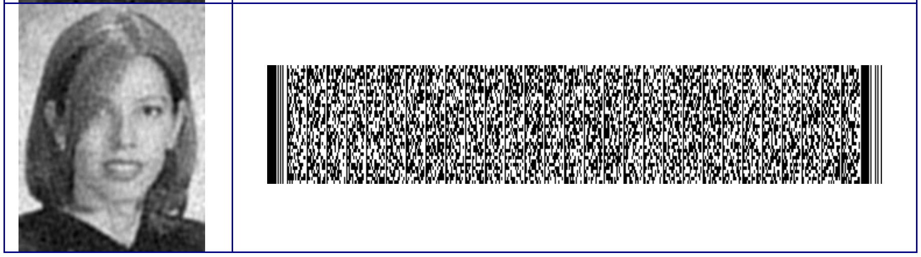


Figure 5 – barcode contains 875 bytes of image data

The Application of 2D Barcodes in Travel Documents

There are several different types of data that can be encoded in a 2D barcode on the data page of an MRTD. When decoded, they provide various levels of document authentication capabilities, and therefore enhance the security and integrity of the travel document.

Text

Perhaps the most straightforward piece of data that can be encoded in a 2D barcode is the 88 characters of text from the machine-readable zone (MRZ) of a travel document (see ***Figure 1,*** page 3). Occupying only 62 bytes of data (compressed at 5.6 bits per character), the information can be decoded at the point of inspection and compared to the textual data visible in the MRZ to detect any alteration via text replacement.

Images

Facial images encoded in a 2D barcode are extremely useful for document authentication purposes. Once an image is decoded, a control authority can compare it with the facial image visible on the document (to verify there has been no alteration or photo substitution), as well as with the traveller presenting him/herself at the checkpoint (to verify that he/she is the rightful holder of the document).

Facial images, however, require significant compression before they can be encoded in a 2D barcode that has a maximum data size of 830 bytes.

The advent of the Internet has resulted in an explosion in the number of images being transmitted electronically, and this has driven the development of various formats for image compression, such as JPEG, JPEG 2000, and WSQ[3]. These commercially available algorithms are very good for the compression of large images, which is what they were designed for. They are, however, inappropriate for the compression of images into very small file sizes, such as what is necessary to fit the facial image on an ICAO-compliant travel document into a 2D barcode.

[3] The best known standard from JPEG, the Joint Photographic Experts Group, is IS 10918-1 (ITU-T T.81), the first of a multi-part set of standards for still image compression. A basic version of this standard is JFIF - what most people commonly refer to as “JPEG”. JPEG2000, a new standard expected to be officially approved in 2001, builds on JPEG but is able to compress images up to 200 times with no appreciable degradation in quality. WSQ, wavelet scalar quantization, is a wavelet transform-based compression standard, originally developed by the United States Federal Bureau of Investigation (FBI) for the compression of digital fingerprint images.

The commonly used JFIF implementation of the JPEG standard, for example, begins to lose its effectiveness as the reduced image size approaches 1 kilobyte. With its large fixed header size (approximately 300 bytes), JPEG images below 1 kilobyte have very little room left for actual data. As a result, JPEG images are largely unreadable at the small file sizes suitable for use in a 2D barcode.

AiT has developed FiCA, an image compression algorithm designed specifically for the encoding of facial images into very small data streams, making it extremely useful for encoding images in 2D barcodes. The algorithm is based on a whole image discrete cosine transform with static Huffman encoding.

As depicted in ***Figure 6***, FiCA version 1.0 performs significantly better than industry standard file formats such as JPEG and WSQ in this application (facial images in the compressed file size range below 1 kilobyte).

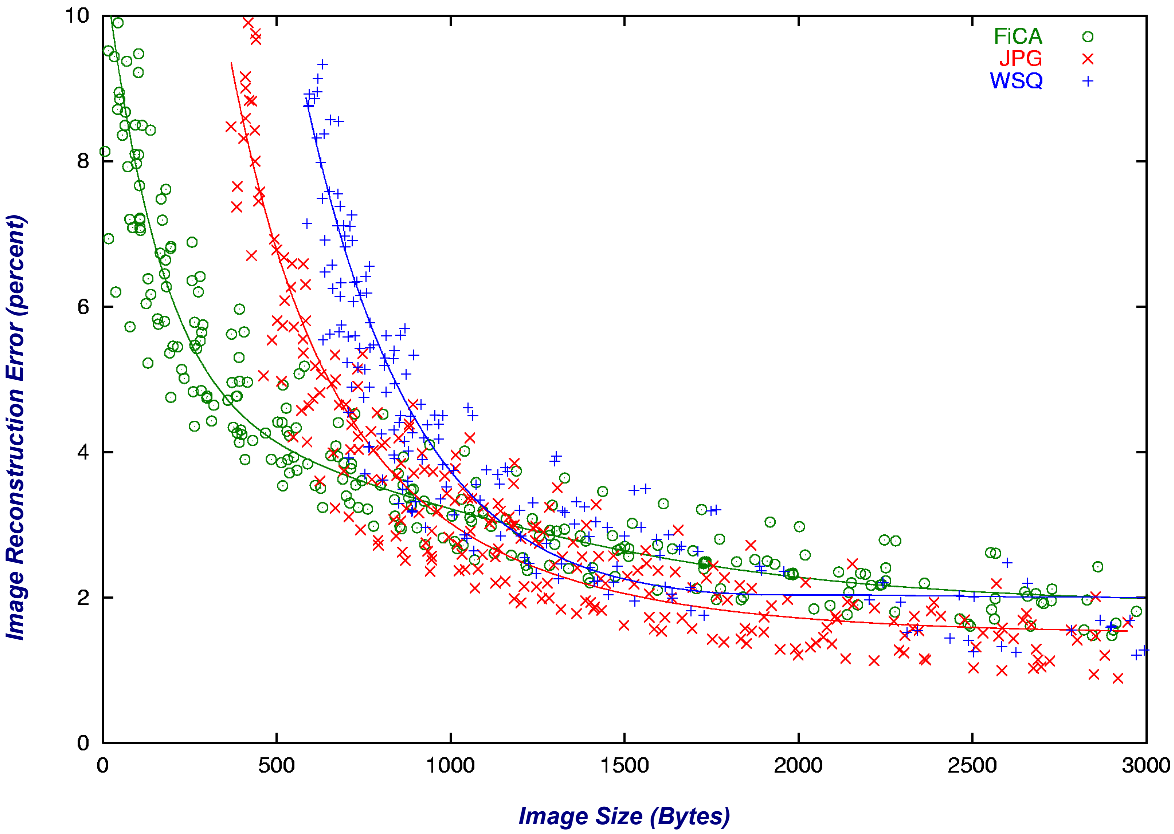


Figure 6 - Mean average error vs. compressed file size for 20 facial images using:

- ***FiCA version 1.0 (Face Image Compression by AiT)***
- ***JPG (JPEG)***
- ***WSQ (Wavelet Scalar Quantization)***

Figures 7 through 11 compare an image in its original format, the same image with JPEG compression, and the same image compressed to three different sizes using FiCA. Even at 482 bytes, FiCA produces an image which is unmistakably the same individual as in the original image, making it effective for use in a document authentication application, as well as compact enough to fit comfortably in a 2D barcode.

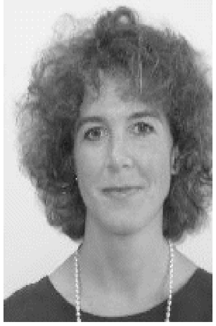


Figure 7 – original image 29600 bytes

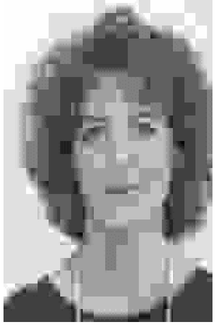


Figure 8 – JPEG format 962 bytes

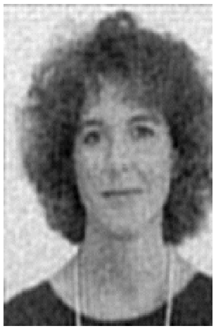


Figure 9 – FiCA 993 bytes

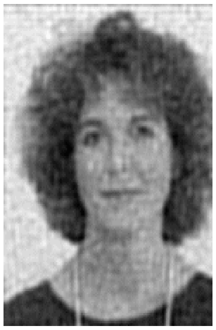


Figure 10 – FiCA 723 bytes

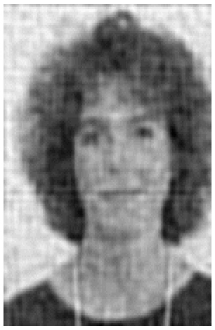


Figure 11 – FiCA 482 bytes

Biometrics

A third data element often used for travel document authentication is the biometric template, normally either a fingerprint or facial image. A biometric template is typically a proprietary data block that contains extra features relevant to a specific biometric algorithm. A biometric template can be encoded in a 2D barcode (a fingerprint template occupies approximately 400 bytes, while the whole fingerprint image would take approximately 100 kilobytes), and then decoded at an inspection point. Using commercial comparison software, the template can be analysed “one-to-one” against a live image, or “one-to-many” against an image held in a database (issuance database, criminal intelligence database, alert list, etc.) to authenticate the document.

Cryptographic Digital Signatures

Digital signatures serve a purpose similar to that of handwritten signatures – they are used to verify the author of a document. Unlike handwritten signatures, digital signatures combine information from both the issuing authority and the document itself. They cannot be copied or “cut and pasted”, and so provide a guarantee of the identity of the issuer. This makes them ideal for use on secure documents such as MRTDs.

The use of digital signatures has become feasible with the advent of Public Key Infrastructure (PKI) systems. A PKI system uses a matching pair of encryption and decryption keys. A private key (accessible only by the issuer) performs a one-way transformation of data that can only be decrypted by its matching public key (made available to everyone). It is virtually impossible to work backwards from the public key to determine the private key.

To form a digital signature, a small representation unique to the message (called the message digest) is mixed with secret information and encrypted using the private key. The public key is used to decrypt the information – if the public key "opens" the digital signature and the message digest matches the message, the identity of the issuer can be guaranteed, as only the public key that matches the private key used for encryption will work.

In the context of MRTDs, a digital signature (approximately 40 bytes) can easily fit in a 2D barcode. When the barcode is decoded and the digital signature decrypted using the public key of the issuer, a control authority can be guaranteed that the document is a valid MRTD from that issuer and not a forgery.

When a digital signature is encoded in a 2D barcode along with other elements – text, facial image, or biometric template, the result is a very secure document, resistant to many different kinds of alteration and forgery.

A Note on Encryption

Cryptographic digital signatures are sometimes wrongly confused with the encryption of other data elements in a 2D barcode. Although it is possible to encrypt MRZ text or facial images before they are encoded, AiT does not recommend this approach unless it is required to meet the specific security needs of an issuer.

Firstly, such information needs to be decrypted before it can be read and analyzed at an inspection point. Since the information (MRZ and photo image) is already visible to the naked eye on the document, it does not seem necessary to "hide" it on the barcode by encrypting it. Most issuers are not concerned about the ability of a third party to *read* a document as long as that party does not have the ability to *change* it. When this is the case, a digital signature will provide the level of security required, and encryption of the other data elements is not necessary.

Secondly, there are legal issues associated with the export of encryption systems from the USA and Canada, requiring costly export licenses and approvals to be obtained.

Printing 2D Barcodes

The proper printing of 2D barcodes is not an easy undertaking and must be integrated with an overall document issuance and printing solution. The use of different types of paper, printing techniques and laminates can affect the readability of the barcode; each component of the total print solution must be considered carefully.

For example, when a barcode is printed, some ink invariably “bleeds”, the severity of which varies with the paper and print methodology. Bleeding makes the black regions of the barcode larger than the white ones, resulting in distorted features, which greatly affects the readability of the barcode. The type of ink used also affects readability of the barcode - 2D barcodes must be printed using ink that can be read under both visible and invisible light.

The choice of security laminate must be carefully weighed. Some common industry laminates do not affect readability, while others render 2D barcodes virtually unreadable. Examples of the effect of laminates on the readability of 2D barcodes are shown in ***Figures 12 and 13***.

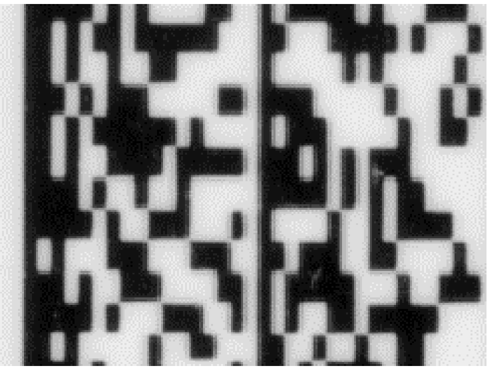


Figure 12 – enlarged section of a 2D barcode without laminate

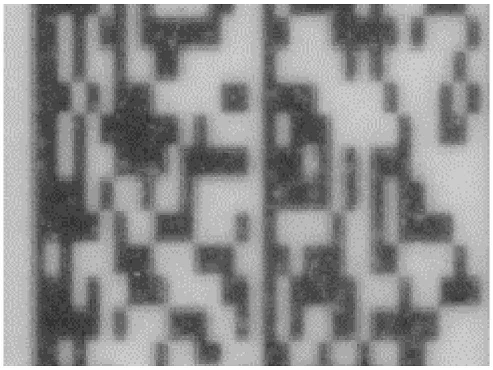


Figure 13 – the same 2D barcode section with laminate

Vendors experienced in working with 2D barcodes, such as AiT, will be able to recommend a document issuance system including a printing solution that optimizes the readability of the barcode.

Reading 2D Barcodes

The security enhancements provided by the inclusion of a 2D barcode on an MRTD are eroded in the absence of an effective way to decode the barcode. The ability to read documents with 2D barcodes at an inspection point must be considered as part of the overall plan for issuing such a document.

Not all MRTD readers are able to read high-density 2D barcodes. Traditional MRTD readers read only the MRZ, but in order to decode a 2D barcode, a reader must be able to scan the "full field of view" of a document and must use specialized software for decoding the barcode. In AiT’s experience, a reader that can achieve a resolution of at least 430 dpi is required to be effective with 2D barcodes.

If a digital signature is to be included in the 2D barcode, a reader must be equipped to decrypt it using a PKI. The most suitable reader, therefore, will hold issuers' public keys in on-board flash memory.

Consideration should also be given to what will be done with the data once it has been collected. Sending such data to an automated border management system can be an effective way to access information in real time that will enhance the security of the entry/exit system.

As with 2D barcode printing solutions, reading solutions need to be carefully chosen. Vendors experienced in reading documents containing 2D barcodes, such as AiT, will be able to recommend a suitable document reading solution.

Summary & Recommendation

With their ability to hold more than 800 bytes of data, 2D barcodes can provide an effective means of authenticating MRTDs.

The forthcoming ICAO standard is expected to outline the use of 2D barcodes on the data page of an MRTD, but will not dictate exactly what kinds of data should be included in the barcode. Issuers will have some flexibility to chose the elements that will provide the desired document authentication capabilities.

To maximize document authentication capabilities, AiT recommends the combination of encoded:

- *text* – to detect alteration via text replacement
- *facial image* – compressed to approximately 500 bytes via FiCA, AiT's algorithm, to detect alteration via photo substitution
- *cryptographic digital signature* – to determine whether or not the document is a legitimate document from the issuance authority

This combination of elements, occupying approximately 600 bytes, fits comfortably on a 2D barcode and provides resistance to many different kinds of attacks on an MRTD, including alteration and forgery.

When issuing a document with a 2D barcode, careful consideration should also be given to what will happen on "the other end". A full implementation plan should include provisions for reading the document, decoding the barcode, and using the data collected.

The new ICAO standard will go a long way toward ensuring consistency in the application of 2D barcodes to MRTDs, however issuing authorities should be careful to choose vendors and solution providers experienced in this area and to adopt technologies that have been tried and tested with secure travel documents.

About AiT

AiT's business is the secure management of personal ID information. Its products are used for the issuance and inspection of secure personal ID documents, and to provide secure access to online personal ID information.