Biometrics in travel and identity documents
A compelling case for physical security features

by James R. Hesse & Charlie Stevens

The critical importance of travel and identity document authenticity goes without saying. The recent introduction of biometrics in such documents, under ICAO’s leadership, takes a significant step in reinforcing document authentication, reducing impersonation and resisting attempts at counterfeit and tampering. Therefore, it would seem that a credential containing a securely stored biometric is the solution to document fraud and there is little need for additional security features on such a document. Nothing could be further from the truth.

If a document reader read every credential that contained a biometric and a live ‘one to one’ verification was conducted then it might indeed be the solution. In reality, 95% of all travel and identity documents that are examined today are not read by an electronic reader. ICAO, however, has never considered biometrics to be a panacea in itself for identity verification but simply to provide an additional security measure for identity in addition to existing secured image and biographical data held in documents.

On the other hand, because these new secure biometric documents are now in widespread circulation there is a serious concern that some examining officers will develop a false sense of security when examining them. It is precisely because these documents are deemed so secure and reliable that they may be accepted at face value without being closely examined. Therefore, although the ‘biometric’ credential makes for a more secure document, if it is not read and doesn’t have front line verifiable features it may actually be less secure than non-biometric documents.

Front line verifiable features
ICAO was mindful of these risks and has retained its promotion of physical security features in its standards for machine-readable travel and identity documents (MRTDs), including biometrics documents. Indeed, ICAO has stated that a biometrics-based travel and identity document should retain all of the physical security features that non-biometrics documents have incorporated and that such documents should still be considered by examining officers as documents verifying identity and citizenship, even if the biometrics chip is non-functional for technical reasons or cannot be read because of a lack of suitable reader. This is a concept described by ICAO as ‘backward compatibility’ and represents an acceptance that biometrics travel and identity documents must be as physically secure as non-biometrics documents. It is important to emphasize that biometrics-based travel and identity documents will not and should not be considered as requiring less physical security or control examination than conventional documents.

ICAO first introduced machine-readable travel document standards in 1980 but even in 2010 some States are still not issuing MRTDs. ICAO introduced biometrics standards for e-Passports and travel documents in 2006 and it is likely that it will take equally as long for global uptake of these biometrics specifications in travel and identity documents by all States. The reader situation is even worse and it is not likely that there will be a universal uptake of standard MRTD or biometrics documents readers at all control points around the world for many, many years to come.

It is therefore essential that all document inspectors are constantly trained to the highest levels to be able to verify credentials by checking physical security safeguards alone. They must be kept fully aware of new developments in document security safeguards so that they can examine and verify the authenticity of credentials with or without readers. They should, of course, where possible be properly equipped with readers so that they can use them in tandem with long-established professional skills in person assessment and document examination.

To ensure that examining officers can reliably and consistently authenticate all credentials, they must continue to contain the highest level of front line ‘eye-readable’ and ‘tactile’ security features. These are proven visual and tactile security features that officers can quickly and confidently rely on.

James R. Hesse has served with the US Federal Government for 34 years in senior positions. James served as a member of the Council of Europe’s Identity Document Committee of Experts, Interpol’s Working Group on Travel and Identity Documents, the International Civil Aviation Organization (ICAO), and G8 Working Groups. He has developed multiple document examination training programs for US and international law enforcement and migration organizations. He currently consults with the US State Department’s Anti-Terrorist Assistance Program and the International Organization for Migration.
Six layers of security
Travel and identity documents should always meet the ICAO content and format specifications, be they in passport booklet or card formats. Such credentials should also be developed by incorporating a ‘layered’ system of security.

• The first layer would consist of front line eye-readable and tactile security features that can be verified with the unaided eye of the examiner and by touch. At this level the security features are very obvious and visual and therefore will be the ones that the counterfeiters will try to replicate. To combat this, these features should ideally be unique to the credential, unique to the document bearer and be of the highest quality of production.

• The second layer should include security features that the examining officer can validate with the use of simple hand-held tools such as a magnifier (loupe) or an ultraviolet light source.

• The third layer would consist of security features that are created during the personalization process, including a ‘swipe’ of the machine-readable zone.

• A fourth layer employs biometrics. A biometric is securely stored in the document, which will then scientifically match the biometric to the bearer when a ‘one to one’ live verification is made using an appropriate reader.

• The fifth layer would incorporate a technology that allows instant access to a database that would contain biographical images and data (a ‘one to many’ identification check), and would also check the document and bearer against a watch list.

• The sixth layer would consist of security features and/or codes that can only be authenticated with forensic equipment. These forensic features for all intents and purposes would be virtually impossible for most counterfeiters to replicate.

This multi-layered approach provides some serious hurdles for counterfeiters to overcome. They can no longer simply scan, reprint and mass-produce credentials. It will be very difficult for them to replicate these documents and have them be creditable at any level.

US Green Card
An excellent example of this layered system in a document is the new US Permanent Resident Card (PRC) or ‘Green Card’ (figures 1 and 2). The card is ICAO-compliant and features not only a range of high quality physical security features but also the proven secure optical security medium (OSM) that contains a biometric. The OSM incorporates some of the most unique, counterfeit-resistant, eye-readable security features available in the world. The PRC features a layering and blending of visual, physical and digital security features. It is manufactured and personalized utilizing a combination of high technology electron beams and silicon diode lasers. During its 10+ years of use in the previous generation PRC, OSM has proven to be extremely difficult to counterfeit and is highly resistant to alteration.

The following points describe the layered security features in the new US Permanent Resident Card:

- Unaided eye-readable and tactile features
  The PRC contains many eye-readable features including optically variable ink (which alternates gold
to green depending on the angle the PRC is viewed at), a highly complex holographic image, tactile images, micro-line security pattern printing and rainbow (or split fountain) printing.

- **Eye-readable security features with basic tools**
  The OSM offers yet another layer of security as there are over ninety extremely high-resolution (24,000 dots per inch) and detailed micro images. When these images are viewed with a simple magnifier the officers will be able to differentiate genuine images from counterfeits due to the quality of the resolution. The PRC also contains fluorescent inks that are revealed when viewed under an ultraviolet light source. Furthermore, there is a latent (hidden) ‘diffractive’ image that can be viewed with a small hand-held tool.

- **Unique personalization features**
  The OSM contains high-resolution, high-contrast eye-readable security features, which are laser etched into the stripe to include the bearer’s photograph, name, signature and other pertinent biographical data. Also, lasers produce a clear tactile personalization of the bearer’s date of birth and gender and there is additional black tactile laser engraving on the front of the PRC.

- **Biometrics**
  The OSM, which can store up to 1.6 Mbytes, is used to accommodate the biometrics in the PRC and contains all digital files and multiple biometrics to include the high-resolution photo, fingerprint and signature of the bearer. The OSM also provides the unequalled flexibility of adding additional biometrics and/or other digital data in the future, i.e. records of dates and location of exit and entry.

- **Database access**
  The PRC uses a Radio Frequency Identification (RFID) chip to instantly access a database that displays the photo image and other biographical information that should appear on the card that is being read. The document and bearer are also checked against a watch list.

---

**Figure 2**
The new US Green Card, back.

**Box 1**

**Case Example: The US Green Card**

*Distribution of the new card by the US Department of Homeland Security (DHS) to legal permanent residents began on 10 May 2010. The Green Card is issued to lawful permanent residents as evidence of their authorization to live and work in the United States.*

The US government has issued more than 20 million optical security media-based Green Cards since 1997. Over this time, the digital security of the card has never been compromised. The new card incorporates progressively enhanced visual and forensic security features and additionally incorporates an RFID tag to provide compliance with the WHTI program, thus facilitating legitimate travel and trade at US land borders. The optical media securely stores digital information including the cardholder’s photograph, fingerprint, name, digitized signature, date of birth and registration number. This information cannot be erased or fraudulently altered and private data can be read only by DHS personnel using secure readers specifically customized for this purpose. The new Green Card is the world’s first implementation of the combination of optical security media and an UHF RFID tag. The customized RFID inlay was developed by KSW Microtec in close co-operation with LaserCard Corporation and is optimized to uniquely match the physical characteristics of LaserCard’s OSM-based credential platform. The resulting new card construction techniques ensure a robust and reliable credential with sophisticated, tamper-proof features. The card also features an optical security media configuration optimized to meet DHS’s requirement for compliance with ICAO standards for ID cards used in travel applications.
- Forensic security features
The PRC contains numerous security features that can only be accessed in a forensic laboratory environment. We are not able to disclose the nature of these features.

A special note should be made regarding the unique security features that are added during the personalization process. The composition of Optical Security Media provides the ability to laser etch very unique features into the stripe. Etched into the OSM are the bearer’s photograph and signature as well as other personal biographical data. These features are unique to each individual card, which virtually eliminates the possibility of mass-producing counterfeit cards. The OSM adds a vital component in the overall approach that the U.S. has taken in the development of the PRC. The PRC is a very secure, counterfeit-resistant document and will prove to be a major problem for the counterfeit document syndicates.

Summary
To summarize, the introduction of biometrics in travel and identity documents is a welcomed and necessary advance in document security but the existence of stored biometrics in credentials should not be viewed as the total answer to document and identity fraud. There continues to be a very important part for excellent quality physical security features to play in biometric credentials. The layered security methodology incorporating a wide range of high-quality and proven physical security features from front line to forensic level will result in the production of the most secure, accurate and counterfeit-resistant travel and identity documents possible. The US Green Card sets an extremely high standard among government identity card programs worldwide and it demonstrates the strength of the layered approach in delivering a secure, ICAO-compliant credential that can be confidently authenticated in multiple scenarios from front line to forensic verification.

If you would like to respond to the contents of this article, please send an email to kjd@keesingreferencesystems.com