

# SECURE DOCUMENT DESIGN

Bruce Monk, Chief Technology Officer, AssureTec Systems, Inc.  
Bruce.Monk@assuretec.com

## Summary:

**An ID that cannot be validated is of no use!** Sole reliance upon data carried by an individual as proof of identity is very weak security. The headlines are full of stories on ID fraud and ID theft. Covert security features too sensitive for dissemination to front-line examiners can be entrusted to a reader/authenticator (assuming it encrypts and protects the criteria and methodology used for to authenticate the feature, such as a data dependent layout or coded cross link between data elements). The inspector needs only to get an overall risk evaluation to combine with their own behavioral assessment to determine if a closer examination is in order. All of the document authentication time can be overlapped with the normal time spent for behavioral evaluation and data checking against databases.

Better ID document design, with close consideration given to what permits effective human inspection and what allows for the fastest, most reliable machine authentication, substantially improves security when the ID is used. People lack the memory capacity to recall a large variety of document properties and the time to closely examine for their presence. Machines have none of the human foibles and, therefore, make the perfect assistant for the inspector and unbiased auditor for the inspector's role in the process. The quality and security of the result directly relates to the quality of the design.

Linking of data elements to each other and to the physical "personalization" process provides the best method for detection of alterations or forgeries. When biometrics and "smart" chip technologies are included in the approach, simple methods can be used for very secure, reliable validation of both the document and the bearer's link to the document without any compromise to the privacy rights of the individual.

**Practical Considerations:** Most identity documents have a life of 5-10 years (some are 50 years!) and others are simply extended by stamping extension data elsewhere in the document. These documents and their challenges will be with us for a long time to come. New verification tools for inspectors will help them greatly; however, a greater openness on issues that add "noise" to the examination process and result in false alerts, lost time, and a tendency to overlook possible fraud indicators, would aid security and reduce net inspection time in a semi-automated inspection process. Recognition that there will be missteps in the rollout of a new design, and establishment of a validation method to resolve the issues in advance, would help both the current situation and minimize the future impact of "OOPS!"

First some broad design considerations:

- 1) Compliance to existing standards.
- 2) Compatibility with existing readers.
- 3) Compatibility with current forensic document examination "tools".
- 4) Minimal re-training requirement for inspectors.
- 5) Distinct security features that do not interfere with photo recognition.
- 6) Print and data protection features that do not inhibit examination of the data by inspectors or machines.
- 7) Less emphasis on deep forensic security features known only to the issuing country.
- 8) More emphasis on security features appropriate to each level of document examination: human unaided, human-aided, machine-aided, forensic expert.
- 9) A country's passport is examined by other countries and validation should be made simpler and more accurate.
- 10) There must be more redundant data checking and cross linking between data elements and between the data elements and the physical properties of the document.
- 11) A primary biometric usable for identity verification should be included (preferably two). Said biometric location should be "tamper-evident".
- 12) A single step process should allow extraction of all information and authentication of the document.
- 13) If a "chip" is incorporated, it must:
  - a. Contain elements to verify the interlinked information characteristics.
  - b. Activate communication only in accordance with a "key" requiring physical presence of the booklet on/in the reader/authenticator.
  - c. Not communicate the biometric information unless a minimum level of authenticity can be established.

In order to ensure interoperability, there should be a formal certification process established for both the document and the reader/authenticators under the auspices of an internationally recognized organization, such as the International Civil Aviation Organization (ICAO).

**Linking Data and Design:** The possibilities are almost limitless if consideration is given to the inclusion of security features or data elements that are linked or intermixed using things like programmable UV colors. All of the above can be combined with some of the variety of techniques used by security printers in the manufacture of currency and passport substrates, such as microprint, Intaglio printing, guilloche, and anti-photo copy processes. The fine line or localized security features requiring laser excitation are best suited for secondary forensic examination. However, if standards were set for specific areas on the passport where holograms, specific wavelength, high energy excitation features, or very high-resolution information can be detected/read, then it becomes practical for reader/authenticator manufacturers to offer options for automated machine verification of the properties contained in that area.

The elements available for establishing these links are:

- 1) Data sub-elements (characters at a specific position in a field or having a particular significance, i.e. birth year from a date field).
- 2) The position of a field or subfield relative to another field, to a registration mark either in the same optical plane or in another plane, i.e. visible vs. NIR vs. UVA vs. UVB.
- 3) Size/type/color/mixture of fonts, images or graphic features.
- 4) Number or inclusion/exclusion of graphic elements.
- 5) Properties of variable images such as photo/fingerprint, i.e. coded representation of image.
- 6) Limits of data values, such as within a certain numeric or alphabetic range.

It is not appropriate to discuss specifics of how these elements might be linked to one another; however, it does not require too much imagination to envision the possibilities of how cross-references or data streams might be developed to make alteration of any element without detection very difficult. Use of all available space and intertwining of data, physical construction, and electronic storage can raise the security bar very high.

**Biometric Technology Drives e-Passports/IDs:** The primary driving force for development of an e-Passport or e-ID is the recognized need for an inspection point to better verify the identity of the bearer of the document as the one to whom it was issued. However, that data borne by the bearer does not necessarily belong to the bearer. Simply including a larger data repository and machine readability does not improve the security of the link between the data and the individual. Actually, as the explosion in identity crime indicates, ready data access compromises security and makes it easier for someone to usurp someone else's data and claim it as their own.

Protection of data on a passport is very different from the challenges faced by the credit card industry or other financial institutions using smart cards. Their losses are purely monetary and get passed on to their customers by way of higher interest rates and fees. Losses from a given source can be "contained" and globally the card can be rendered unusable.

In a travel document, use of the smart chip can be stopped by a few seconds in the microwave or inadvertently through "normal" failure or environmental hazards. The fallback process must be to rely on the physical document. It is very naive to believe that the hacking of the digital "signature" properties sufficiently to allow simulation "spoofing" of a valid authentication will not occur very quickly, if the value versus cost proposition warrants.

The driving force for choosing chip technology over multi-dimensional barcodes, for example, was the reliability of reading the many kilobytes of data (currently specified as 32 kilobytes minimum for the e-Passport). Originally it was anticipated that the state of biometric standards would allow for the storage of biometric "templates" and, hence, much more biometric information and perhaps visa or other transaction log type information could be included. Instead only lossy compressed images of the face and a fingerprint (or two) can be accommodated. The transfer speed was anticipated to be an improvement over current technology but actually it will be significantly slower until technology improves to allow reliable transfers at higher rates.

Perhaps the single greatest barrier remains the issue of interoperability of chips and biometric templates. Progress is being made, but the path remains long. This is not a disparagement of the technology, or of its potential. It is a simple assessment of where we are in its development and its role in the design of a highly secure document. None of these design discussions would be relevant if secure, real-time validation of a traveler's captured biometric by the issuer of the passport were possible. This is unlikely to come to be in my lifetime. It is a real possibility for consideration within the jurisdiction of the issuer.

**Overcoming Space Limitations:** There are several ways to overcome the issues of space limitations for biometric storage. It is important to remember that human vision extends approximately from 400nm (blue) to 700nm (red). Common ultraviolet (UV) excitation is centered at 365nm (UV-A, long-wave), 311nm (UV-B, medium-wave), and 254nm (UV-C, short-wave). Near-infrared (NIR) excitation extends from about 800nm to 1 micrometer. These frequencies are all in use today in the design of passports.

Optically variable devices (OVD: holograms, kinegrams, crystograms, etc.) and optically variable inks basically employ different techniques to reflect/absorb light when excited from visible light at a particular incident angle. Said light returned to the view point may vary in intensity, color, or both.

The basic elements in construction of a Data Page (DP) are the substrate (paper, plastic), the personalization information, and an overlay. The personalization information maybe placed on the substrate or the overlay, and security features may be present on any or all elements. The basic DP dimensions are about 5" (125mm) wide and 3.4" (86mm) high. The diagram below gives the basic space allocations as set forth by ICAO-9303 [REF].

**A Layered Approach:** Great progress has been made in the area of stable specialty pigments for inks, dyes, and toners. Other areas include solid-state light sources, and solid-state image sensors (camera chips) and the associated processing power to provide powerful imaging capabilities. Related to these, but in a different part of the electromagnetic spectrum, is RF technology, particularly that associated with embedded materials that provide a unique "signature" when excited in a carrier such as the substrate of a passport or potentially even in the ink, dye, or toner.

The general concept is simply to layer the construction of the passport using different excitation sources and/or coatings for isolation to provide as much physical space as needed to contain the information needed. All information would be human visible with readily available instruments. Security would come from either areas isolated for human visible specialty devices or from the way in which the information is coded and laid out according to the data contents. There is no need for barcodes to hold actual data since all information can be presented in clear human/machine visible formats.

As an example, a high quality image can be printed on a white background without any interfering patterns in the background, merged, or overlaid on top. Said image, if printed with continuous tone properties at 600 dpi, would exceed the quality requirements for biometric comparison. A fragile overlay would be used to provide tamper-evidence. Further security in the region could come from redundantly printing the photograph using IR absorbing clear inks, layered with NIR transparent visible inks, and a continuous tone UV-A for good measure. These images could be registered to each other and vary in size or location according to data parameters. Further protection could come by printing or engraving a small isolated "thumbnail" or "ghost" image elsewhere on the DP. The "ghost" image could further be protected by an OVD (overt feature) or up-converting/down-converting ink (covert feature). The Canadian passport and others already incorporate personalized UV printing and transparent NIR inks are now available. Any or all of the images can be printed on top of one another and used for biometric comparison purposes. However, a simple graphic "template" can be stored as a small barcode or in a chip and extracted from the image on the passport for validation. It could also be centrally stored by the issuer and validated upon request.

There are no issues of lighting, pose, aging, varying expression, or factors such as: glasses, facial, hair, or makeup when comparing the region as a graphic versus a facial match. Better yet, there is no privacy issue, since the graphic template would be of no use in identifying a person. Said template would be small and could be freely distributed or on-line validated by the issuer without sharing any privacy information. It simply represents extraction of a seal or key to confirm that the photo on the document is the one placed there by the issuer. Digital watermarks could serve the same purpose but standardization and proprietary issues become an issue with virtually no added benefit.

A similar approach could be taken with the machine-readable zone (MRZ). The two MRZ lines of a passport could be printed in visible NIR transparent Ink/Toner/Dye (ITD) and a duplicate printed offset from the visible version using transparent NIR absorbing ITD, perhaps according to parameters derived from the check digits. ICAO compliant readers would read the NIR version and people could read the other. Another available option is to accomplish the same thing using UV fluorescing ITD.

Outside of the photo area and the MRZ, the remainder of the document is available for data or other images. It is recommended that OVDs not be used to "protect" the data. Their use in areas not to be viewed by man or machine to extract information is fine, and can be human or machine authenticated. In particular, use of any materials which hurt the resolution or distort the information they were intended to protect, should be avoided. This includes materials such as 3M's Confirm laminate whose glass-bead properties tend to de-focus and reduce contrast for visible, NIR, and UV images.

**Easier for Humans and Machines to Read:** As an example, full compliance with ICAO-9303 recommendations for the Human Readable Zone (HRZ) can be met, as can a country's interests in presenting a unique, recognizable national image. The challenge is to accommodate them both while making it easy for a human or machine to view the data for cross-checking against the MRZ. In addition to the ICAO specified data, specific text or graphic indicators can be added to cross-link and verify the integrity of the data. Very strong consideration should be given toward the use of data dependent layout parameters. Such layout factors can automatically be measured by full-page reader/authenticators and cross-compared against data such as stock number, issue date, issue location, or expiration date. Any data on the booklet could be used directly or indirectly as a parameter to subtly vary the layout.

A known problem associated with fraudulent passports is stolen materials. Theft may come through collusion by an insider, during storage, or during transit. For the most part, there is currently no reliable way to machine-read the stock number while viewing the document. A new design can provide for cross-referencing the stock number to an embedded intrinsic property at the time of manufacturing of substrate. This property could be the RF “signature” of a substrate with embedded RF reflecting materials, or the pattern of embedded UV fibers, or both. The RF signature would be less subject to tampering, but require specialized reader capabilities. The RF signature could also provide another layer of security that could be registered and cross verified, either by comparison against a version stored in a small barcode, on a chip, or with the issuer. This signature does not present any privacy issue, so it can freely be linked to the Document number and graphic template without violating any privacy laws.

The detection of patterns of document usage, apart from collecting or sharing any personal identifiers, does not represent any invasion of privacy. In the case of a perceived risk, then the issuer or a recent transaction point, where the data is still legally held, may be queried. This also minimizes the amount of benign information that could clutter a database.

We still have many options and a great deal of space available. So for a passport, why not print two rolled, 500 dpi, 256-level grayscale, FBI-compliant fingerprint images in the Human Readable Zone using clear NIR or UV ink/dye/toner in reverse on the data page side of the overlay? If NIR ink/dye/toner is used, this could also be done as step one in a two step process of printing directly on the data page.

**Conclusion:** There are issues to consider relative to document wear and aging. However, building a document issuance strategy that allows for production of an e-Passport/ID that protects the information in electronic storage with physical attributes of the document, and crosschecks the data with enough information to make evident any alteration, is a much needed tool in the fight against identity crime and its support for terrorism, drug trafficking, etc. When combined with a viable fallback strategy and technology to get the most out of exiting passport/DL/ID during the years of transition, then we are on our way to better securing our borders while protecting the privacy of our citizens.

A more open policy on the dissemination of exceptions during the production of existing ID documents, and the ability to real-time validate the issuance of an ID with a specific number on a given date at a specific location without any personal information, would represent minimal security risk and go a long way toward improving today’s border security. Though the data is not contained in the MRZ, a current generation reader/authenticator can reliably read this information wherever printed on a passport.

Hence, automatic validation that such a document was legitimately produced, combined with close machine examination for evidence of tampering or forgery, further lowers the risk that at least the passport is real. Automatic location and magnification of the photo area and negation of obstructions, such as OVDs, dramatically improves an inspector’s ability to verify the link between the bearer and the document. The next step is utilization of Automated Facial Matching (AFM) to aid/alert the inspector of possible fraud or match against lists of known “undesirables.” If there is questionable behavior, suspicion that the bearer is not the person to whom the document was issued, or if there is a question of document authenticity, then clear risk is proven and referral to a secondary inspection point is in order. This is not an endorsement of facial matching as a preferred biometric for the future; however, it is the reality of what is currently present on the identification documents in circulation today and for some time in the future.

## References

- [1] James Hesse, “Counterfeiting and Misuse of the Social Security Card and State and Local Identity Documents,” Testimony before U.S. House Judiciary Committee, Subcommittee on Immigration and Claims, July 22, 1999.
- [2] Gary Thomas, “Bush Administration Asks for Extension of High Tech Passport Deadline,” Voice of America News, March 24, 2004.
- [3] American Association of Motor Vehicle Administrators (AAMVA), Personal Identification – AAMVA International Specification – DL/ID Card Design, September 25, 2003.
- [4] International Civil Aviation Organization (ICAO), Document 9303, Machine Readable Travel Documents, Part 1 — Machine Readable Passports (2002), Part 2 — Machine Readable Visas (1994), Part 3 — Size 1 and Size 2 Machine Readable Official Travel Documents (2002), ICAO, Montreal, Quebec, Canada.
- [5] Asa Hutchinson (Under Secretary DHS), Testimony before U.S. Senate Committee on Finance, September 9, 2003,
- [6] Drivers License Guide Company, ID Checking Guide, 2004 Edition, Redwood City, CA, 2004.
- [7] Bruce Monk, “Designing Identity Documents for Automated Screening”, 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21-22, 2004.
- [8] Theodore Kuklinski, “Automated Authentication of Current Identity Documents”, 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21, 22, 2004.