

BUILDING BETTER SECURITY INTO IDENTITY DOCUMENTS

January 24, 2004

INTRODUCTION:

Purpose of an Identity Document: Identity Documents (IDs) exist in order to establish a link between the bearer of the document and their right to goods, services, or a privilege, such as crossing a border or entering a building. The document evolution started hundreds of years before the ability to include a photo of the bearer. Therefore, the early documents carried information which described the bearer, i.e. height, weight, hair color, eye color, or distinguishing features. The document also conveyed the name of the bearer and, by its endemic characteristics or written instructions on the document; who issued the document; and what the intended use was for it, i.e. license to drive, passport, membership, etc.

The legitimacy of the document was established by unique visible properties of the document and attested to by an official “seal” or “signature.” Alteration or forgery of such documents is about as old as the use of such devices. The challenge today remains the same as it did from the start. The first is to prove positively that the bearer of the document is the person to whom it was legitimately issued and then it is to establish that the rights conveyed have not been revoked officially or “de facto” by fraud in obtaining the document or by actions taken by the individual that override the granting of rights/privileges at the time/point of a transaction. The intent is to minimize the risk associated with the transaction. This proposition of proving Link and Legitimacy in order to Reduce Risk will be referred to herein as LL-RR.

The Tradeoff: The quest for convenience and speed has always been the trade-off with the level of security in the transaction. The value of the transaction set the level of security that was built into the document and the degree to which the authority granting permission examined the document and bearer to establish authenticity. At one time this could take days or weeks as a “trusted” advocate was sought to attest to the identity of the individual or the validity of the document! Evolution always leaves traces of the past and that is true with the many “legacy” features of the documents and methods that we use today for LL-RR.

The fact that there is new technology which appears to offer great potential improvements in LL-RR should be evaluated with caution. Seldom does “re-invention” work outside of strong consideration for the huge inventory of information both in physical dimensions and in the knowledge and training of the personnel. The road of recent history is littered with the burned chassis[?] of great projects intended to re-invent. Success comes from careful planning to firmly establish the true goals and objectives along the way and a clear understanding of how and why things are being done the way they are today.

Security Precepts: Identity documents are a role player in the quest to improve security. It is important to keep in mind ten security precepts:

- 1) Know your threats (who, what, why).
- 2) Know your vulnerabilities (where, when, how).
- 3) The best security is prevention in advance of “attack” through intelligence.
- 4) Layered or multi-level security is most effective.
- 5) Static security features are more vulnerable than dynamic ones.
- 6) Address the basic or simplest threats first to thwart the lowest cost/risk attacks. This represents the best return on investment.
- 7) As you remove the lower level vulnerabilities, you can increasingly focus resources on narrower, more specific threats.
- 8) As you accomplish 7) you raise the cost and risk of detection for the attacker.
- 9) Human vulnerabilities are the highest risk factor.
- 10) Deny access to information, travel, and needed materials/services and you will prevent serious attack.

The Threats: The first precept above, “Know your threats (who, what, why),” is critical to answer when prioritizing resources and scheduling tasks. There are four basic threat levels or categories of threat:

- 1) The “amateur” who has minimal resources and experience. Their purposes are generally associated with personal goals, such as illegal immigration or travel. If caught, these people have little risk of the consequences and often will try many times.
- 2) The “professional facilitator” who makes a business out of aiding people in the Category 1, but sometimes aid those in Category 3. Though much better equipped and experienced, they lack sufficient capital to invest in the materials and equipment necessary to alter or forge documents with a high degree of accuracy. They have little risk of being caught and the consequences are not much more than for the “amateur.”
- 3) This category represents the “professional criminal” element. These are the drug traffickers, smugglers, less organized terrorists, “people” traffickers, international thieves, etc. Though they sometimes use the “professional facilitator” when the risk is perceived to be very low, more often they fund their own or share “trusted” false document operations. The available funding is much larger and their risk, if caught, is much greater. Often these organizations use “mules” traveling under fabricated identities to avoid their own complicity.
- 4) The highest threat level is posed by foreign governments or “quasi-government” terrorist organizations with broad access to funding, resources, and intelligence. The most proficient of these often have their own laboratories and regularly resort to criminal activities to infiltrate their target. This may be theft of materials, bribery, blackmail, or intimidation. If detected, the consequences toward achievement of their intended goals may be catastrophic; hence, the return on their investment is much greater.

It is very important to note that the sheer volume of identity fraud represented by threats in Categories 1 and 2 makes detection of Category 3 and 4 document fraud activities much harder. The impact of each individual incident of document fraud in the first two categories may have much less economic impact or represent less physical threat. However, when taken in aggregate,

the net economic impact is much greater and the assistance provided to threat levels three and four is a major contributor to increased security risk.

In order to focus resources on the higher threat levels, we must first minimize the success rate for the lower levels. This is largely a matter of overcoming the obstacle presented by a desire to spend-less and process faster at the point of document inspection. This is the point at which automation of the inspection process can offer the maximum benefit. Automated document inspection and identity verification tools at the inspection point will simultaneously improve the security level and reduce the required processing time.

Document Design Precepts: Consideration of the ten security precepts is critical to the design of a good identity document. They are also critical to the implementation verification process needed to deal with the newly designed documents in an environment dominated by the legacy of existing IDs. It is quite a legacy! There are hundreds of millions of existing ID documents from several thousand issuers. Each issuer may have several variations and several generations of a document, all valid at the same time.

There are several ID design/verification principles that parallel the precepts for general security. They are:

- 1) Consider: Who would want to forge or alter it; what would they do; and why would they do it?
- 2) Consider: Where, when, and how would they attack the ID?
- 3) Evaluate and/or share information on:
 - a. lost/stolen documents or materials/devices used for production of IDs
 - b. trends or methodology being used for alteration/forgery
 - c. unique ID features/properties
 - d. an ID identifier (issuer/number) prior to its use at the transaction point
 - e. ID usage patterns
- 4) Use/verify multiple security features: overt/covert both machine- and human-readable/verifiable
- 5) Change some ID characteristics often and publish the changes to the inspection authorities and/or secure manufacturers of ID verification devices. In addition, or alternatively, offer a validation service that checks information collected from the ID, but protects the criteria used for confirmation
- 6) First design the ID for easy human readability and verifiable features (albeit static ones!), then provide layers of features for human and machine examination, each of which is interlocked to the other. Protect data and biometric (photo, et al) by interlocking them to the physical characteristics of the ID.
- 7) The greater the perceived risk at a transaction point, then the more detailed forensic examination of ID, physical screening of the bearer, and the background checking of the individual. Check the basic layer ID and bearer name; only if there is perceived potential risk go deeper and validate using combinations of data and validation of ID versus issuer records (no need to obtain the data itself from the issuer unless there is a sufficient perceived threat to justify it).
- 8) It takes specialized expertise, materials, and equipment to produce an ID which has tightly coupled the data, image, and security features with sufficient quality to pass a

well-design verification process. Access to these components incurs substantial cost and risk of detection, as does the process of obtaining or forging “breeder” documents needed to fraudulently obtain real ID documents.

- 9) Any good process for issuance of an ID or verification during the LL-RR must accept that human participation is the greatest risk of all and minimize the impact! While people are essential and, for some situations unmatched by any machine, they are very vulnerable to:
 - a. Poor training/memory
 - b. Distraction
 - c. Bribery
 - d. Physical Intimidation
 - e. Blackmail
 - f. Fatigue
 - g. Disillusionment (unhappiness with home, work, or life in general)
- 10) Denial of access to travel, facilities/materials, and information of great value to criminals is the role of the ID and the ID verification process. Provision of information on critical behavior patterns and, in advance of transactions, is the promise of closer integration into the security paradigm.

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.

History and Future: The International Civilian Aviation Organization (ICAO) Travel Document specification ICAO-9303 is described in a paper entitled “Guidelines to ICAO-9303” jointly authored by John Mercer and John Hotchner (Passport Services, U.S. Department of State) and Gary McDonald (Canadian Passport Office). This paper does a good job of covering the background and purpose for the standard’s development. The effort to gain international adoption and subsequent compliance has been monumental and, unfortunately, not completely successful today, 18 years later. However, the need is even greater today than it was then. International travel has increased many fold and continues to grow. Much of this travel increase is coming from emerging countries. This increases the diversity of the traveling public and, hence, many more language and cultural backgrounds need to be considered.

Along with the increase in travel and tourism has come an explosion in global commerce. These positive effects of technology’s impact toward “shrinking” our planet have also brought another type of explosion. Global crime has increased even faster! International terrorism, flight to avoid prosecution, illegal migration, and illegal traffic in persons, drugs, goods, and stolen property are among the crimes aided by Identity Fraud and Identity Theft.

AN APPROACH TO SECURE DOCUMENT DESIGN:

Purpose: What is described herein is intended to provoke discussion and stimulate thought. It represents public disclosure of intellectual property and, thereby, negates the protection of that property. If the concepts presented are the property of any other person or organization, I apologize. They are being presented without knowledge of such proprietary constraints and in the interest of moving forward in the evolution of identity documents. Passport design will be

used as an example, though most concepts are applicable to all security documents. Hopefully, conflicting governmental and commercial interests can be set aside and consideration be given to the merits of a broader thought process. It is not intended to be “anti” any particular technology, but rather to put in perspective a holistic view of how the pieces might fit together cooperatively.

Looking Forward but Remembering the Past: Certainly any new design should maintain backward compatibility with existing standards and the primary methods for reading and authenticating them. This basically comes down to human observation and machine-readability via the International Civil Aviation Organization (ICAO) Machine Readable Zone (MRZ) as specified in standard ICAO-9303 (ISO-7501). Basic constraints such as the data elements, photo location, and the general recommended space allocations for each element should be preserved. The evolution of the e-Passport specification to add “smart chip” capabilities as an option does not constrain this discussion. The current pending specification for the use of “smart” chips in a passport is limited to the broad physical parameters and more specific data formats, communications protocols, and data elements (currently photo and one or more optional fingerprints, and the data as contained in the MRZ) needed for global interoperability.

The “chip” is viewed primarily as a repository for electronic data representations of the information and photo on the Data Page for cross-checking. The specification also provides for optional storage of additional biometric image(s) for potential future automated biometric verification of the link between the bearer and the passport. The complexities of trying to internationally administer data encryption “keys” and other data security schema have precluded protection of the data with the types of schema. A digital “signature” is proposed, but its relative merits as a global security device will not be debated herein.

The ICAO has made it very clear that the “Data Page” remains the primary source for information and security evaluation. This paper is referenced to the design of the Data Page; however, the general concepts are applicable to any design for a secure document. Many new security technologies have emerged over the last few years. The main objective in establishing ICAO-9303 was to bring order to chaos. Machine-readability and a generally consistent format were dictated by the unacceptably long time required and high error rate associated with manual data extraction and examination of documents. The type of data, language, and location of data and photo varied from country to country and from generation to generation of document.

The data check digits included in MRZ lines were intended to detect OCR errors at a time where the technology was just emerging. Since it was not viewed as a security feature, the check digit algorithm is published as a part of the specification. However, detection of possible data alteration has been greatly improved by verification of these check digits. Unfortunately, many countries purporting to have machine-readable documents do not comply with ICAO-9303. Common discrepancies include improper fonts, incorrect check digit calculation, incorrect line spacing, lack of near-infrared absorbing ink, and variability in the photo location. Even within a specific country there are often wide variations in the printing of the MRZ between production locations and over the production life of a passport. There are no real specifications on the variety of “security features” a country uses on a passport. Nor are there constraints on the potential conflict between examination of the photo or reading of the data in the human-readable zone and the security features intended to protect them.

It would be a tremendous help to border inspectors, with no degradation in security of the passport, if the issuing country would simply make available what physical characteristics the MRZ on their documents should have if printed at a specific time over a date range. Realizing that exact times may not be available, even general ranges of possibilities would help. Also, the practice of allowing locations to continue to issue passports, using obsolete stock and print methods after a reasonable period of time passes, should end immediately.

Practical Considerations: This current dilemma is mentioned by way of a backdrop for the environment which a new passport design will have to coexist. Most passports have a life of 6-10 years and some are simply extended by stamping extension data elsewhere in the passport booklet. These documents and their challenges will be with us for many years. 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 impact future “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 passport.
- 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 passport and the reader/authenticators under the auspices of an internationally recognized organization, such as the National Institute of Standards and Technology (NIST) in the United States, SITA, or ARINC.

Biometric Technology Drives e-Passports: The primary driving force for development of an e-Passport is the recognized need for a country to better verify the identity of the bearer of the passport as the one to whom it was issued. It is a fact, 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 fall-back process must be to rely on the Data Page. It is very naïve to believe that the hacking of the digital "signature" properties sufficiently to allow simulation 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.

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 will certainly not 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 while achieving the design objectives. 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 (holograms, kinegrams, crystograms, et al) 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.

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 the 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 passport 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 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 it was intended to protect, should be avoided. This includes material 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: 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 DP. A new design can provide for cross-referencing the stock number to an embedded intrinsic property at the time of manufacturing of the DP 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 Passport 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 why not print two rolled, 500 dpi, 256-level grayscale, FBI-compliant fingerprint images in the HRZ using clear NIR or UV IDT in reverse on the DP side of the overlay? If NIR IDT is used, this could also be done as step one in a two step process of printing directly on the DP.

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 prints 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.

There are issues to consider relative to document wear and aging. However, building a passport issuance strategy that allows for production of an e-Passport that protects the information in electronic storage with physical attributes of the DP and cross-checks the data with enough information to 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 passports 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 passports, and an ability to real-time validate the issuance of a passport 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 passport was 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.

Conclusion: Covert security features too sensitive for dissemination to front-line examiners can be entrusted to the 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 passport authentication time can be overlapped with the normal time spent for behavioral evaluation and data checking against databases.

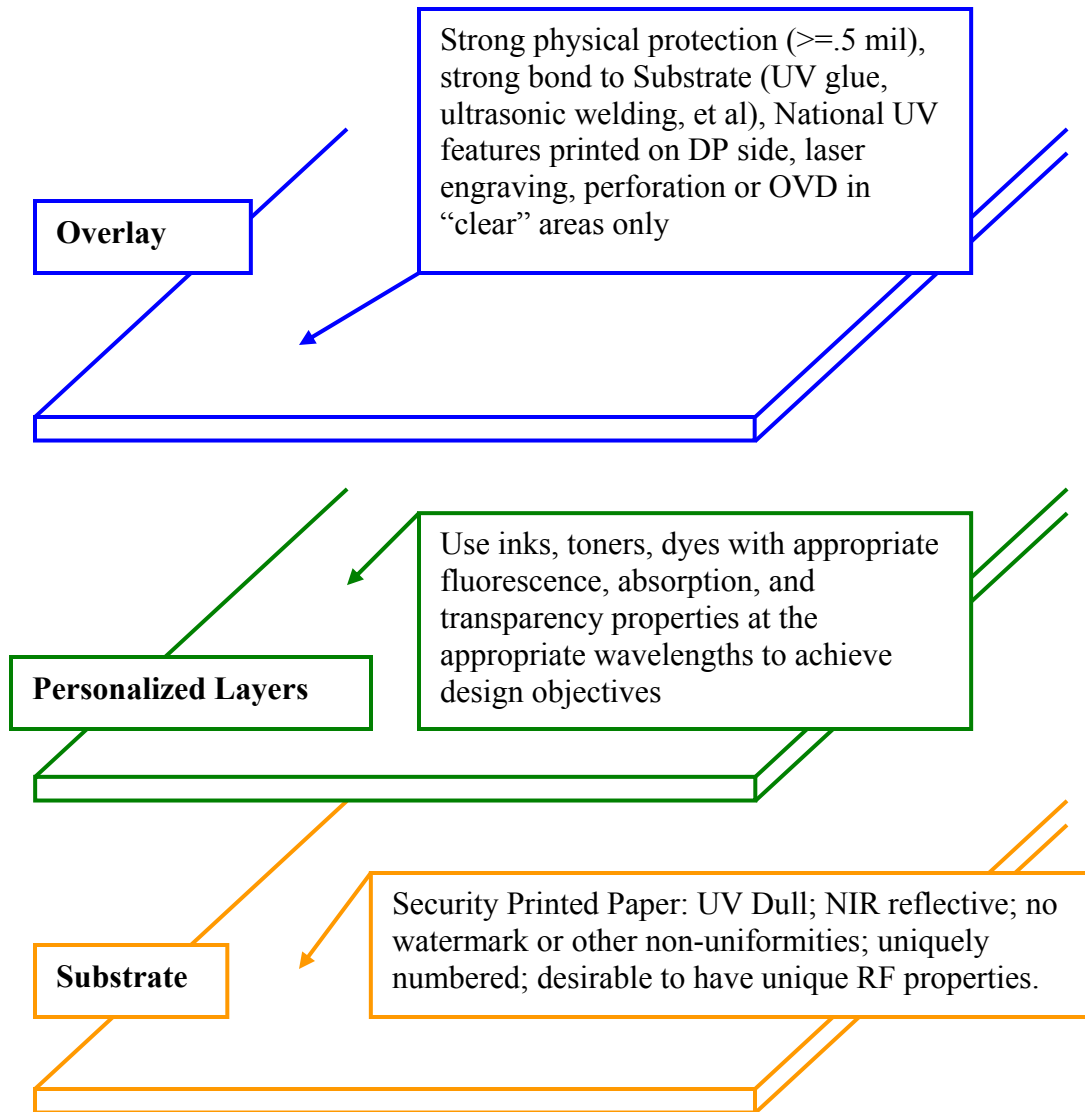
Better passport design, with close consideration given to what permits effective human inspection and what allows for the fastest, most reliable machine authentication, substantially improves security when the passport is used. People lack the memory capacity to recall a large variety of document properties 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 of the result directly relates to the quality of the passport design.

APPENDIX

- A) Layered Construction**
- B) Isolate Areas of Interest and Stack Data/Security Features**
- C) Example of Linked Data Coding**
- D) Illustration of Linked Graphic Symbology**
- E) Illustration of Data Dependent Layout Schema**
- F) Preserving the National Persona and Protecting Privacy**
- G) Computing a Photo “Signature”**
- H) Forensic/embedded “track and trace”**

APPENDIX A: Layered Construction

Layered Design Provides More Space and Security Options



APPENDIX C: Example of Linked Data Coding

Linked Data Coding (LDC) can be thought of in much the same ways that “check digits” are used for detecting errors in a string of characters. The concept is simply to construct a string of characters based on Key (often altered) Characters (KC) from data elements such as Name, Date of Birth, Expiration Date, Issue Date, Issuing Location, Sex, and Document Number.

Said LDC consist of characters derived from the serial combination of the KC from each data element carried over to the next and so on with the final link back to the starting character.

FOR EXAMPLE:

GIVEN:	1) Last Name	=	Jones
	2) First Name	=	Jonathan
	3) Birth Date	=	25-08-1948 (dd-mm-yyyy)
	4) Issue Date	=	15-10-1978
	5) Expiration Date	=	25-08-1988
	6) Issuing Location	=	Boston ...
	7) Sex	=	Male
	8) Document Number	=	150496281

CHOOSE:

1) Next to last character	=	e
2) Second character	=	o
3) Decade	=	4
4) Second digit day	=	5
5) Second digit month	=	8
6) Last character city	=	n
7) Second character	=	a
8) Fourth character	=	4

THEN:

- A) Add ASCII character position (1-26) for 1) to character position for 2)
 - a. Result = $5+15 = 20$
 - b. Use **2** as first character in LDC
 - c. Carry units digit, 0, to next step
- B) Add carry digit from A) to 3) = $4 + 0 = 04$
 - a. Use **0** as next LDC character
 - b. Carry units digit, 4, to next step
- C) Add carry digit from B) to 4) = $4+5 = 09$
 - a. Use **0** as next LDC character
 - b. Carry units digit, 9 to next step
- D) Add carry digit from C) to 5) = $5+8 = 13$
 - a. Use **1** as next LDC character

- b. Carry units digit, 3, to next step
- E) Add carry digit from D) to character position for 6) = $3+14 = 17$
 - a. Use **1** as the next LDC character
 - b. Carry units digit, 7, to next step
- F) Add carry digit from E) to character position for 7) = $7+1 = 08$
 - a. Use **0** as the next LDC character
 - b. Carry units digit, 8, to next step
- G) Add carry digit from F) to 8) = $8+4 = 12$
 - a. Use **1** as the next LDC character
 - b. Carry units digit, 2, to the next step
- H) Add the carry digit from G) to the character position for 1) = $2+5 = 07$
Use **07** as the last digits of the LDC

RESULTS:

LDC =200110107

Some alternate approaches could be:

- 1) Offset ASCII characters by including 0-9. Therefore, the character position for “a” would be 10.
- 2) Use base-32 arithmetic
- 3) Weight/offset the results of each step by a step dependent amount

BENEFITS:

- 1) Easily human verifiable with any change to one of the selected characters indicated by a break the link.
- 2) The location of the “break” indicates which data element has been altered.
- 3) The LDC may be shared or remotely validated by the Issuer of the document without any violation of privacy
- 4) Readily stored on “chip” or Barcode

APPENDIX D: Illustration of Linked Graphic Symbology

Linked Graphic Symbology (LGS) is the practice of using a graphic symbol(s) or number/characters to represent a link to a data element or data element range. This is most useful for providing a coarse range for first/last letters of names, birth date ranges, issuance date ranges or sex.

POSSIBILITIES:

- 1) Print a series of Characters or Symbols (CS) and have just one position represent the sex.
- 2) Print an arrangement of CS and have the number/position indicate the alphabet range for the First/Last Name
- 3) Print a string of 7 CS that represent the binary equivalent of the birth year.
- 4) Print an arrangement of CS that cross-reference a layout option for text, photo, or graphic

FOR EXAMPLE:

- 1) An even or odd number of flags could be male/female

Female



Male



- 2) Flag upright could mean male or tilted female

Male



Female



- 2) Binary year of birth, expiration, or issue could be coded by presence/absence; or tilted not tilted

Birth Date = 1986



- 3) Third letter of a Name field:

A-H =



I-P =



Q-Z =



- 4) Orientation of flag above could indicate the expected first character position for a field or top-right location of the photo.

APPENDIX E: Illustration of Data Dependent Layout Schema

Data Dependant Layout (DDL) is the practice of changing the position and/or size of text or graphic elements according to data values. Location of a field or data within a field may be varied. The size/type of font or the photo location or size could be varied.

If done on a “row-column” grid, the first character in the data or the field label would represent the “registration point” for that element. The locations may be referenced relative to each other or to a fixed registration mark(s).

FOR EXAMPLE:

See how many variations for the basic Layout 1 below are illustrated by Layout 2

Layout !

Name of the Issuing State			
Passport	Type	Country code	Passport number
Passport holder's photograph	Family names		
	Given names		
	Nationality		
	Date of birth		Personal identification
	Sex	Place of birth	
	Date of issue		Issuing authority
	Expiration date		Holder's signature
MACHINE READING AREA			

Layout 2

Name of the Issuing State			
Passport	Type	Country code	Passport number
Passport holder's photograph	Family names		
	Given names		
	Nationality		
	Date of birth		Personal identification
	Sex	Place of birth	
	Date of issue	Issuing authority	
	Expiration date		Holder's signature
MACHINE READING AREA			

Given the 15 layout elements that are not rigidly established, and the fact that the field label as well as the data within the field can vary, a 3 character horizontal grid range and a 2 position (.5 line spacing) vertical range, there are 30 to the 6th power or 729,000,000 combinations. Add the NIR and UV layer possibilities and there are almost limitless choices for layout variants. All of these variants should readily handled by a full-page reader authenticator without any knowledge of the significance relative to the data content.

If the reader protects the algorithm for validating the layout then all of the measurements needed to determine the validity of the document can be made and only a "risk factor" needs to be presented to the operator. The level of this cooperation is up to the Issuer.

APPENDIX F: Preserving the National Persona and Protecting Privacy

Standards and standard practices permit interoperability and human inspection of a document from lots of different Issuers. However, the passport is an official document from a sovereign nation charged with protecting its citizens. The challenge is to provide security while protecting privacy.

It is very important to remember that all countries have the same basic responsibilities to its citizenry and have to operate under a system of law that is intended to provide the guidelines needed to meet those responsibilities. It is unreasonable to expect that one country can expect another to ask that it change laws or add burdens unless they are prepared to do the same.

An Issuer should have the freedom to “personalize” their ID document, if the intended use, identity verification, is kept in mind. Often the document is a strong statement of national pride and the value of the privilege that is granted by the document is imparted by the unique quality which it displays.

The design of a passport should allow a country to express its national pride and unique persona. However, it should express these while keeping in mind that the ultimate accolade comes from meeting the intended use with maximum ease of use and maximum security regardless of the inspection process, no matter where it is presented.

There has been much presented in other sections relative to doing the job well. What has not been expanded upon is the opportunity that is available in the background printing, header area at the top of the DP, and in “open” areas where very visible security features such as OVDs and laser engraving can be used to both add security, but also reinforce uniqueness. On the inner layers (UV, NIR), as well, country specific elements can be included to set apart the passport.

The obligation to protect the citizen from invasive processes and associated hassles can be accomplished if the passport is the person that is recorded and tracked and not the person linked to it! If the properties of the passport are measured and validated at the highest levels according to standards of quality and construction, then one level of security is achieved. Consistency, redundant data, durability, and tamper evidence are major contributors at this level.

At the next level machine-readability extends this to a deeper level by expanding the variety and complexity that can be included. At the deepest forensic level, positive covert discriminators can provide positive evidence of the heritage of the document.

By creating a unique, strong and easily validated “documetric” for the passport (or any ID document), the burden then shifts to the link between the bearer and the document at the point of presentation. Given the strong protection of the biometric(s) of the bearer, that bearer-document link can be locally verified in several ways:

- 1) Eye-viewable high quality unobstructed photo and fingerprint images where permitted and biometrics can be cross-verified in various ways (UV, NIR, and “chip”).

- 2) Automatic machine-readable comparison from multiple sources with automatic tamper detection.
- 3) Remotely validated by the Issuer or a “clearinghouse” without any invasion of the privacy of the bearer through confirmation of the graphic code for the photo area and the LDC.

APPENDIX G: Computing a Photo “Signature”

The photo placed on an identity document is more specific than the facial biometric for the bearer of the document. It is a specific instance of that individual’s face. It has unique lighting, hair style, expression, background, clothes, and pose characteristics. It would be extremely difficult to reproduce that precise photo even with the same individual available for the picture!

The uniqueness of the photo makes validation of the photo a much simpler task than a facial match to the bearer of the document. There are several ways to create a digital signature for the photo. Each would yield a code similar in concept to a biometric template, but without the need for the measurement accuracy or complexity to establish the likelihood that the photo is the one that was placed on the document at the time of its creation.

Most techniques will obliterate the relationship between the person in the photo and the code that represents the “signature” for the photo. Thereby, any link to the individual is destroyed and, along with it, any privacy concerns.

It is not the intent of this paper to cover specific design details, so certain broad claims are made without addressing exactly what is necessary for the approach to be robust. Among the measurements that might be used to generate the code are:

- 1) Statistics of different sub-regions.
- 2) RGB, CMYK, intensity profiles/slices.
- 3) Derivatives or integrals of the above.
- 4) Wavelet coefficients.
- 5) Histogram analysis.

Obviously, registration marks and color calibration areas would aid robustness/precision. However, even without these features, cross-correlation techniques will allow validation of the photo to the original with a degree of accuracy that will eliminate undetected photo substitution.

The measurement technique can be published and the validation against the original issue can be linked with other data on the document and/or it may be validated by the Issuer. This would be a very fast means of verifying the photo on a passport without recalling a large image file from a chip for visual comparison. This technique is of particular interest if a country wishes to offer a validation service without compromising privacy. It also answers the important question of how to preserve the link between bearer and document, without compromising privacy, while being able to track the activity associated with the document.

APPENDIX H: Forensic/embedded “track and trace”

There are many options emerging for providing the positive covert forensic level needed by law enforcement to provide the documetric equivalent to what DNA offers as a biometric. The capture and registration of unique characteristics for individual documents at the time of their manufacture/personalization can accomplish this.

As with the use of other security features, multiple layers offer the best way of ensuring that no attempt at alteration or forgery will go undetected at a forensic level. This process can be made more certain by deliberate introduction of deterministic properties into the document as a class and individually.

Amongst the candidates for providing this level of protection are:

- 1) Embedded, encapsulated DNA from plants.
- 2) Particles randomly embedded in the substrate or elsewhere which offer a unique RF, UV, or IR “signature”.
- 3) Microscopic profiling of specific areas where unique fiber, ink, or “tool” structures may be observed.
- 4) Deliberate, personalized, irreversible engraving, etching of the substrate or over-laminate.