HIGH SECURITY IDENTIFICATION DOCUMENTS

Using QSDC to Determine the Right Mix

By Nick Nugent
Datacard Group

DatacardGroup

For anyone involved in the production of a high security identification document — whether a driver's license, national ID, passport or other — the risk of the program is a constant concern. Will the document look good and hold up after years of use? How do we make it affordable? Can we make the document easy to verify yet ensure it will resist deliberate criminal attack?

In this article, Nick Nugent delivers a new framework for considering and evaluating key trade-offs in selecting and designing a secure identification program. This framework articulates a step-by-step process for determining the right mix of Quality, Security, Durability and Cost (QSDC) to manage that risk.

INTRODUCTION

Quality, Security, Durability and Cost (QSDC) are the cornerstones of any successful Identity Document (ID) program. These criteria have trade-offs and compromises, and the relative value of each must be considered when designing the most appropriate ID. This article defines critical elements of ID programs, identifies real-world challenges and provides the reader with the knowledge necessary to overcome these challenges using proven best practices to minimize the risk to any ID program.

Quality: A high-quality document will be consistent in appearance and closely match all other documents issued in the same ID program. The security features — in particular, the primary portrait — will be crisp and clearly defined to allow easy authentication. Machine-readable features, such as chips, optically readable characters (OCR) and barcodes, will read consistently and accurately. Laminates will have the necessary optical clarity. Overall, a high-quality identity document will look and feel like one.

Security: The security of an ID is a measure of how well it resists deliberate attack. Document attack is either by simulation to produce a counterfeit, or by tampering in an attempt to alter the information within the ID. The security of the document depends upon how difficult it is to simulate or tamper, and also how easily the genuine document may be verified as being genuine.

Durability: The durability of an ID defines its resistance to change. A document is exposed to a variety of environmental hazards during its life, such as light, flex, extreme temperatures and humidity. It may also be subjected to accidental attack —— such as laundering — or deliberate misuse, such as using a card for something other than intended (e.g. scraping ice off a windshield). An ID with high durability will survive the required validity period without significant visual change, and without compromise to its performance.

Cost: The cost of the document refers to the cost to produce it. This will include the fixed and variable costs associated with enrollment, manufacturing, personalization, issuance, shipping, and the many administrative functions necessary to manage and secure these functions.

THE CHALLENGES

The elements of QSDC are under constant threat. For an ID to function and survive in the "real world," it must be threat resistant — achieved by careful design with QSDC in mind. Materials, components, features, hardware, software, processes, procedures and training must all play a part in delivering an ID document that successfully meets the performance challenges.

Figure 1 - The Challenges to ID Performance

It is important to appreciate that QSDC are not simply just linked together, they are inextricably entwined around each other. Any change in the performance of one criterion will have a ripple effect on others. This article now examines each of these cornerstones in turn, and considers how to effectively produce and manage the right mix.

QUALITY – MEETING THE CHALLENGES

A high security ID is usually a national, or even international, document. Its quality reflects the quality of the issuing authority and the holder ought to be proud of it. However, the quality of an ID is also linked to its performance, security and durability.

1. **Poor quality leads to variations between documents, which makes simulation easier and verification harder.**
   The essence of security printing is the mass production of identical documents. Be they banknotes, passports, ID cards or tickets to the World Cup Final, the genuine articles must all look the same so that counterfeits, with their minor imperfections, can be identified. A person who inspects an ID document is, in effect, attempting to "spot the difference". He/she has just seconds to answer the question: "Does the document in front of me look different than the genuine document?"

Quality — or more specifically in this case — consistency, must persist throughout the entire process of ID document production. In particular, manufacturing and personalization processes must ensure consistent "close match output," so that all genuine documents look sufficiently similar to make a counterfeiter's task more difficult.

2. **Unreadable machine-readable features, such as a chip or OCR, make documents vulnerable.**
   There has been a large increase in the use of machine-readable features for ID documents in recent years. Such elements certainly add new challenges for the criminal, particularly when used to complement the physical security features. Biometrics is a good example of a technology that can help protect ID documents. However, these features can be expensive and there are often pressures to deliver a solution at the lowest possible cost. Biometrics can also be a false economy, jeopardizing the security of the document if there are insufficient physical security features backing them up, should they fail. Purposefully damaging chips so the biometrics are unreadable has also been a tactic used by criminals. If the chip is the only security feature associated with the ID, and it doesn't function, it causes the examiner to make a "judgment call" rather than a more informed decision of authenticity.

3. **Low quality components erode security.**
   The majority of security features on an ID document are not machine-readable. These "human-readable" defenses function best when they are clear and unambiguous, which can be jeopardized by low quality components. If overlays are hazy, a polycarbonate does not engrave cleanly, or if Optically Variable Devices (OVDs) such as holograms are blurred and ill-defined, then verification doubts can arise.

4. **Low quality components or equipment could reduce durability performance.**
   A decision to select components of low quality is unlikely to be made consciously; however, lower quality may very well be a consequence of cost cutting. Not all vendors offer the same quality of substrates, inks, overlays, holograms, etc., and equipment performance can also vary. The result may be an ID that begins its life looking fresh and new, but all too quickly succumbs to the durability challenges of the real-life ID.

Achieving the necessary quality requires several factors, including design, QC processes, calibration and maintenance. In particular, material components and system hardware should not be selected independently of each other. The quality of the issued ID is likely to be at its highest if the materials and system have been matched, designed and tested together to ensure optimised output.

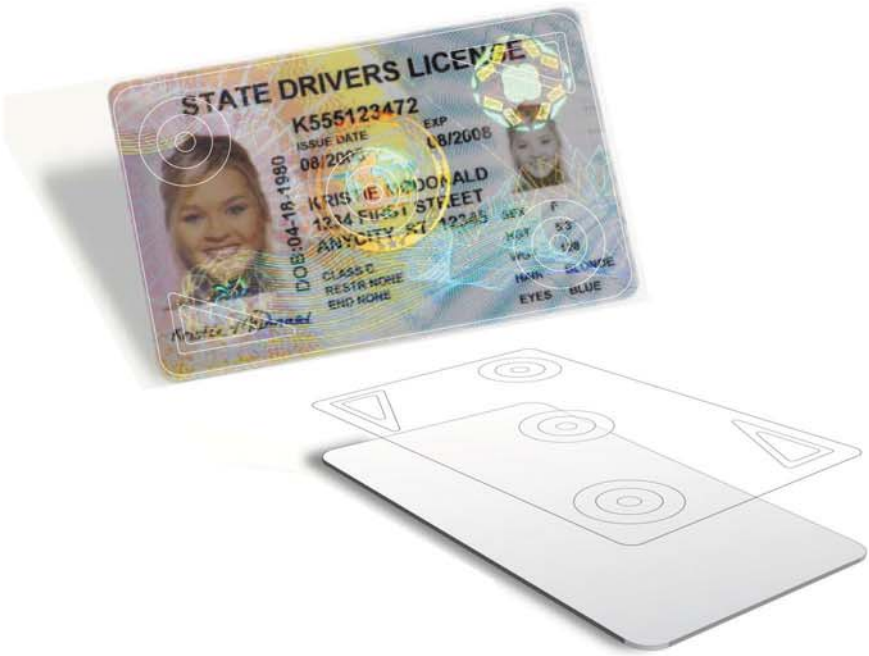


Figure 2 - Sample Drivers License
Design identity documents using the multilayered security approach.

Achieving the necessary quality requires several factors, including design, QC processes, calibration and maintenance. In particular, material components and system hardware should not be selected independently of each other. The quality of the issued ID is likely to be at its highest if the materials and system have been matched, designed and tested together to ensure optimised output.

SECURITY – LAYERED DEFENSES

Layered security and the use of multiple security features (overt, covert and forensic) is a fundamental principle that needs to be carefully considered when designing an ID program.

1. Security features

Criminals attack IDs in many ways, broadly described as either simulation or alteration. The role of security features are to highlight to an inspector or examiner, such as a policeman or an immigration officer, that an attack might have taken place and then — through closer inspection — provide sufficient evidence that confirms the initial suspicion. For this reason, security features are not just difficult to simulate, but must also be easy to verify.

Because attacks are many and various, no single security feature is capable of defending against them all. Instead, a layered network of security features should be incorporated into the ID.

The easiest features to verify are overt Level 1, which can be verified without a device. This is in contrast to covert Level 2 and forensic Level 3 features, which require knowledge and a device to verify. The hidden security offered by Level 2 and 3 is an important aspect of the layered network of defenses, and may deter counterfeiting; however, most inspectors ask for at least two strong Level 1 features in ID documents.

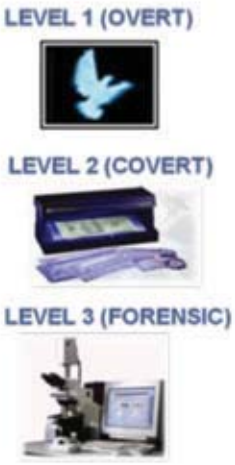


Figure 3 - The Use of Security

The strongest security features:

- Encourage inspection by giving the examiner something interesting to look at and look for
- Allow quick, confident decisions on authenticity
- Are unambiguous and intuitive
- Do not need a tool or device
- Utilize the variable biodata
- Cannot be effectively simulated using commercial materials/equipment
- Are tamper evident

It is an advantage if the genuine security feature has been created using materials and equipment that are not commonly available. However, this does not guarantee strong security. It is important to remember that the criminal is ingenious, and might use relatively low-tech methods and materials to copy features or effects that have been created using complex, high-tech and expensive processes. For example, the counterfeiting of a security hologram might be done using a different hologram removed from a different document, as long as the colors and effects are similar. Or, the simulation of basic laser engraving might be achieved with black digital print, rather than a laser. Complex optically variable effects have even been simulated using furniture polish or cosmetic make-up easily purchased in beauty supply stores.

2. Security at Time Of Personalization.

Another aspect of security features is where they are located in the document. An ID is formed of many components and assembled in many stages. For comprehensive security, the features should be designed to occur throughout the document.

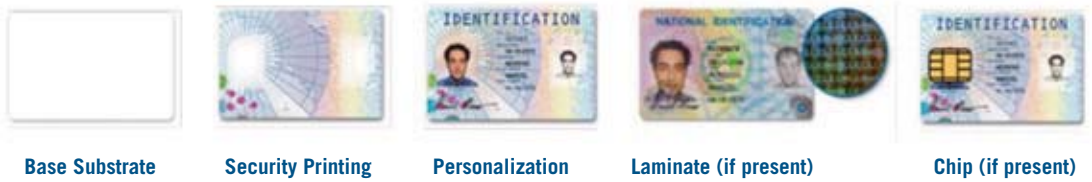
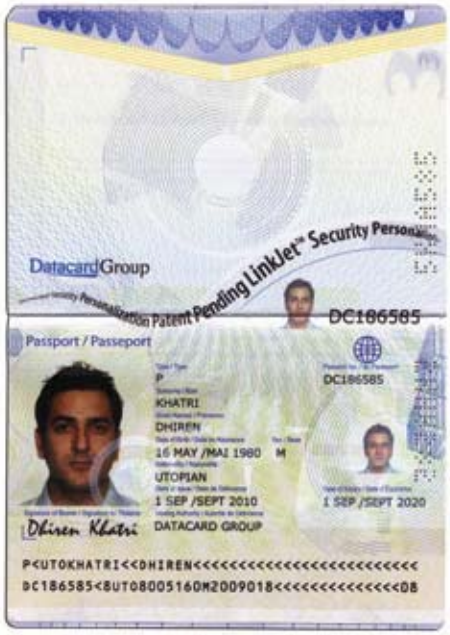


Figure 4 - Security Throughout the Document

The least effective security features are those the criminal can easily acquire. Watermarked paper or holographic laminate may be very difficult to counterfeit, but can also be stolen. By using these stolen components, those very same properties that make the feature strong now support the fraud and validate that the counterfeit document is genuine. By arranging security features throughout the document, theft of any particular component is of less value to the criminal. This is particularly true for features created during personalization.



By bringing together during personalization all the elements necessary to create the feature, it becomes more challenging for the criminal to recreate or acquire it, and thus security is improved. Personalization data, restricted materials, unique engineering and process secrets can all combine in very strong synergy to make the task of counterfeiting significantly more difficult. Security at Time of Personalization features have the added advantage of also defending against data alteration.

Certain personalization technologies further enhance tamper-resistance by penetrating the substrate: inkjet permeating into passport paper and laser engraving of suitable polymers are examples of personalized data being held deep beneath the surface of the card or passport data page.

Figure 5 - Security at Time of Personalization

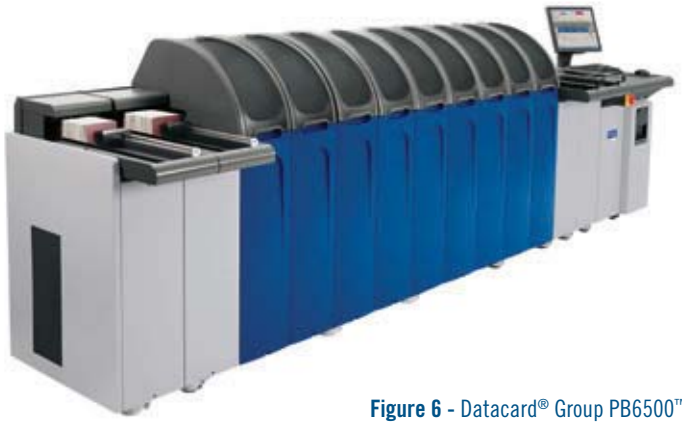


Figure 6 - Datacard® Group PB6500™ Passport Issuance System

3. Beware the "silver bullet".

The industry has many vendors that describe their technology or feature as being the only defence necessary to provide total security to an ID. Experience has found that this is never the case. The dangers of reliance on any single feature are clearly illustrated when considering the strengths and weakness of the smart chip.

Although there are many reported cases of hacking of the chips within electronic IDs, most of these stories do not stand up to scrutiny and turn out to be just media hype. The reality is that chips are highly resistant to duplication or data alteration, as long as the necessary layers of defenses have been implemented. Much excellent work has been done in the last 10 years by ICAO, Smart Card Alliance Association and others to ensure that the development of electronic security remains at least one step ahead of the criminal.

However, even the chip does not represent a "silver bullet". Readers cannot always be relied upon and are not always available. Chips and readers break, and may be deliberately disabled so that they do not function correctly, or at all. Even electricity can be intermittent in many developing countries.

Unfortunately, there are several examples of governments reducing the budget for traditional physical security features of a document in order to afford the smart chip and the system infrastructure to read it. When a citizen arrives at a border with a passport and the smart chip does not function, the immigration officer must scrutinize the physical security features. But what if these features have been downgraded in order to pay for the chip, and those that remain are less reliable? What if the document requires further evaluation in a back office? The citizen is inconvenienced and security may be compromised.

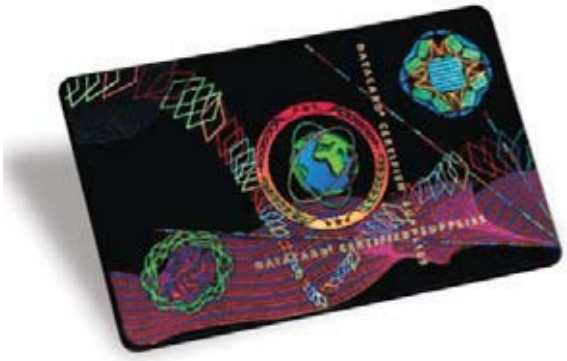


Figure 7 - Overt, Covert and Forensic Features Should All Be Considered When Designing a Secure ID

4. Design and training.

Holistic design of the ID document is a critical part of successful, cost-effective security. A security feature that is to be incorporated into one of the various layers of a document (substrate, printing, personalization, laminate, chip, etc.) needs to be designed with full consideration of the likely threats and other defences. For example, addition of a forensic taggant to the substrate might increase counterfeit detection, but offer little tamper evidence.

Furthermore, a feature designed in isolation may have its effect compromised by other features or components in the document, or may be duplicating other defences and thus, offer a low return on investment. For example, security laminates may contain optical effects that are reduced by the underlying print design, or an anti-scanner feature such as optically variable ink may duplicate the anti-scanner properties of an integrated holographic device. Consider a successful sports team, where the coach gets the most out of the players by getting them to play as a team and not as a group of individuals.

The challenge is to coordinate several different designers, often working in several different vendors' studios, to ensure a team approach is achieved.

Training is also essential. The best security features in the world are of no value if the examining individual lacks the skills necessary for accurate verification. A program of training and awareness helps ensure that everyone who might need to make a decision on the validity of a document both knows and cares about the features within.

DURABILITY IN THE REAL WORLD

The concept of "normal use" for an ID document is open to interpretation. A passport may be used to travel across borders, and also to open a bank account, this is normal. However, what if the passport is sat on for 150 days a year by a busy business traveller, or accidentally passes through a washing machine, or falls in a puddle of oil? And what is normal use for an ID card — to be carried around in a pocket with keys and coins and inserted daily into a reader, to be worn as a badge in bright sunshine for 200 days per year, or to be kept in a drawer at home and rarely, if ever, taken into the outside world?

The point is that an ID needs to be designed to resist all the environments that it might reasonably encounter. Laboratory testing of specific performance criteria — such as flex, bend, delamination, abrasion, solvent attack, lightfastness, humidity, etc. — can ensure that certain durability standards have been met. These standards have evolved over many years, and continue to do so. There are many that are used to provide guidance in the setting of durability performance, including:

- Durability of Machine Readable Passports Version: 3.2, TF4, N0232, 2006-08-30
- Identification cards – Physical Characteristics, ISO/IEC 7810
- Identification cards – Test Methods, ISO 10373-1/6
- Card Durability Test Methods, ANSI, January 2007
- Identification cards – Card Service Life, Part 1: Application Profiles, ISO 24789-1
- Identification cards – Card Service Life, Part 2: Methods of evaluation, ISO 24789-2

The release of the new ISO 24789 – Card Service Life standards will enable governments to more closely specify an application profile that fits their unique situation. Past test standards have not allowed for specific use case analysis in developing a set of recommended test protocols. Developing unique profiles will ensure tests meet customer durability requirements.

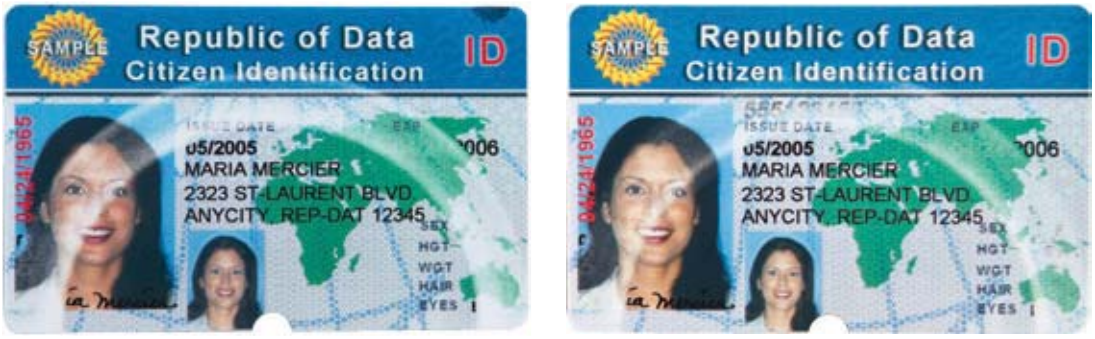


Figure 8 - Laboratory Taber Tests Evaluate Durability of Cards

It is important to remember that results of these tests may provide important insight into the likely performance of an ID. However, it is up to each issuer to set pass/fail criteria for these tests. Also the real world is a more complicated place than a laboratory, and the durability challenges faced by documents are not able to be precisely reproduced in the lab, where accelerated testing and extrapolation must be used to predict performance over many years. In short, there is no substitute for experience in the use of particular materials, construction methods and personalization technologies in order to minimize the risk of an ID failing in normal use.

A further complication is introduced by the need to reveal if attempts have been made to alter the document using physical or chemical attack. For this reason, laminates must be sufficiently tough to survive for many years, yet delicate enough to break if attempts are made to lift them intact. Examples where physical and chemical weaknesses have been designed into the document to highlight tamper can be found in passports. The introduction of micro-perforations or delicate cuts within a laminate or visa sticker and the use of low-peel strength passport paper both challenge the criminal to remove the laminate or visa in one piece without damaging the page beneath.

Chemical detectors may be introduced in the form of tiny dye particles within the paper that are designed to bleed, visibly, if it is subjected to the solvents that might be used to lift laminates or visas.

These features must, of course, remain dormant when faced with the rigours of "normal use," and only activate if tamper has been attempted.

COST-EFFECTIVE PERFORMANCE

In an ideal world quality, security and durability would be maximized and implemented without a consideration for cost. In reality of course, budgets are limited and there are constraints. A government department must fight for the funds to deliver the best possible system to its population, and the citizen must be offered the document at an affordable price. This is especially true for mandatory ID card systems, where citizens must, by law, have been issued a card for which they will be expected to pay. With over one quarter of the world's population living in poverty on less than $2 per day, there will often be a gap between cost of the document and ability to pay.

Although the challenges of finite budgets are all too clear, the risks of making a difficult situation worse by cutting costs in the wrong areas are less obvious.

Saving money on design or security features is usually a false economy; poorly designed or weakly protected documents may suffer mass fraud, thus requiring expensive re-design and even a new issuance program. The use of poor quality components — such as substrates, inks and chips — shortens document life and again may end up costing even more money than doing it right in the first place.

Perhaps the biggest danger comes in the use of a single expensive feature, such as a chip. There are examples where this has reduced spending on the overall layered network of defenses, leading to a lower security document. It is not always clear if a government reduces spending on security features because they have to or because they think they no longer need such features as they now have a "silver bullet". As we have already seen, the single impregnable security feature does not exist in the real world.

The most important factor in implementing a program within budget is to learn from other people's mistakes. The use of tried and tested best practices helps minimize the chance of unexpected overspending.

Considering best practices in the early stages of a secure identification project and overlaying these recommendations with the unique needs of the individual project enables stakeholders to ensure compliance with local, regional and international standards and practices. In addition, they realize higher security, obtain greater

efficiency, lower risk and receive acceptance from all stakeholders in the final document and process.

The generation of best practices is perhaps the most important recent evolution of the industry. The maturation of technology and the development of standards have led to mass adoption of secure identification document programs and this adoption has created a rich environment for generating best practices. Sources of best practices include other governments, experienced organizations and vendors, and, importantly, documentation from industry groups such as ICAO, AAMVA, APEC, GlobalPlatform, and the Smart Card Alliance. Understanding the lessons learned in other projects allows for early consideration and identification of key topics ranging from issuing organization structure and project management consideration, to end-user concerns, to supply chain optimization and security, and even specific technology recommendations.

While all projects are unique, frameworks and tools exist to map best practices to specific project requirements, add confidence to the decision-making process, and ease the implementation process. Together this approach ensures the highest level of success in complex identification programs.

Figure 9 - Secure ID Solution Overview

SUMMARY

QSDC are critical parts of a successful ID program and, as demonstrated, have a strong linkage to one another. When selecting the provider(s) of an ID solution, it is essential to understand the trade-offs presented in the QSDC framework to help reduce the risks associated with issuing secure identity documents.

There are many solution providers that have the necessary experience to deliver secure ID programs to government organizations. The most successful programs and solutions providers utilize best practices and a broad portfolio of integrated solutions (hardware, software, supplies and service) that work together to enable government organizations to find the right balance of QSDC — the right mix — for their secure ID program.

SG12-6001

DatacardGroup

CORPORATE HEADQUARTERS
11111 Bren Road West
Minnetonka, Minnesota 55343-9015
Phone: +1 952 933 1223
www.datacard.com
info@datacard.com