Secure Identity Technologies

Advanced identity solutions for government agencies and system integrators

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

Secure identity solutions 3

Higher efficiency, greater security, lower risk 3

Quality, Security, Durability, and Cost (QSDC™) 4

Personalization technologies 6

Personalization security features 8

Overlay material technologies 14

Overlay security features 16

Digital technologies 18

Technology-printer matrix 19

Glossary of terms 20

Secure identity solutions based on industry standards and proven best practices

Government agencies around the world trust Entrust to provide a range of secure identity solutions, including national IDs, passports, driver's licenses, personal identity verification (PIV) cards, entitlement IDs, and more. They choose Entrust because our solutions are designed in compliance with industry standards and they offer strong physical and digital security. Our solutions also provide insights, developed through deep experience with government identity programs in hundreds of national, regional, and local government engagements worldwide. Entrust can recommend best practices that result in maximum efficiency, lower risk, and greater security. As a result, government agencies we serve produce identity documents that are secure, effective, and well-respected by citizens and the international community.

Higher efficiency, greater security, lower risk

A trusted government solutions provider

Governments around the world trust Entrust to provide highly secure identification solutions for cards and passports through innovative technologies, products, and services.

We have spent decades working to build secure, efficient issuance solutions using innovative technology that strengthens security and adapts to constantly changing threats. Our portfolio includes hardware, software, supplies, and services, and we understand the processes required to comply with standards and ensure the highest levels of security.

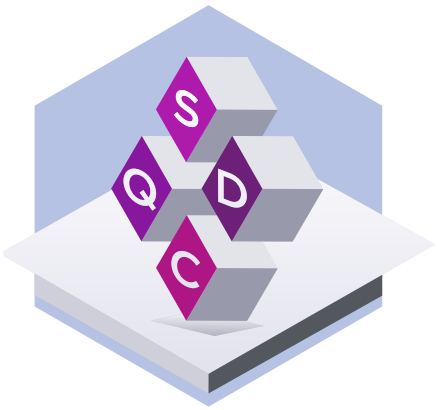
Historically, the majority of physical security features found on a passport, national ID, or other identity document were added during the blank document manufacturing process, prior to personalization.

Security at the Time of Personalization™ (STOP) is a design strategy that adds key elements to the credential during the personalization process. This makes supply items less desirable to counterfeiters and enhances the overall security of the document. Many of the security features discussed in this brochure can be integrated as part of an effective Security at the Time of Personalization initiative.

Whether your project involves passports, national IDs, driver's licenses, entitlement cards, or any other document with an expectation of security, you can trust Entrust. We will bring valuable insights to your identity program:

- **Global experience.** More than 400 projects in over 100 countries.
- **Best practices.** For improving security, maximizing efficiency, and reducing risk.
- **Comprehensive portfolio.** Physical and digital solutions for the secure identity process.
- **Collaborative approach.** Our identity experts work side-by-side with you.

The anatomy of a secure credential



Quality, Security, Durability, and Cost (QSDC) are the cornerstones of any successful identity document (ID) program. These criteria offer benefits and trade-offs that must be considered when designing a credential for a specific program.

The elements of QSDC are under constant threat. Materials, components, hardware, software, processes, procedures, and training must all play a part in ensuring the credential delivers on its original design goals.

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 bar codes, 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. Counterfeiters may exploit weaknesses in the credential's design to alter, augment, or destroy its integrity. A growing number of cases involve a genuine document being presented by a look-alike fraudster. Security features that exhibit tamper-evidence and include multiple portraits can help protect the document.

Durability: A government credential is exposed to a wide range of stressors over its lifetime, including exposure to light, temperature extremes, and flexing. It may also be subjected to accidental attack – such as laundry – 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 wear, and without compromise to its performance.

Cost: Most credential programs consider the total cost of the ID, including the fixed and variable costs associated with enrollment, manufacture, personalization, issuance, shipping, and the many administrative functions necessary to manage and secure these functions. Cost per document business models are becoming more common.

When the government team makes key decisions about their new credential, it's more than likely involving a trade-off between these four considerations.

Level 1-2-3 (Overt – Covert – Forensic)

Experts classify security features into three different categories: overt, covert and forensic, or Level 1, 2 and 3. Newer ISO standards have refined this thinking, but the original concepts are still helpful in considering new security features.

	Description	Examples
Level 1 – Overt	Visible to the naked eye or to other human senses such as touch, and requires little or no training to verify.	• Cardholder Portrait • Color Shifting Ink • Tactile signature • Watermarks • Holograms
Level 2 – Covert	Hidden element until a common tool is used to reveal it, such as a magnifying glass or special lighting. Some knowledge or training is required to verify.	• Ultraviolet printing • Infrared printing • Smart Chips • Temperature sensing inks
Level 3 – Forensic	Deeply hidden forensic feature. Requires knowledge, expertise, and advanced laboratory tools to verify (microscope, chemical analysis)	• Nanotext • Substrate analysis

Most credentials are designed with a mix of Level 1, 2 and 3 security features. The Level 1 features are especially helpful for those who need to inspect the document quickly, such as border officials.

Personalization Technologies

PRINTING

Direct dye sublimation printing

Dye diffusion thermal transfer (D2T2) – also known as dye sublimation – is the most common method of card personalization today. It uses thermal printhead technology to transfer dyes directly to a suitable substrate, providing near edge-to-edge coverage.

Applications: D2T2 printing is typically available in 300 dpi image quality using three- or four-color monochrome or paneled print ribbons. Dyes must be protected with an overlay or laminate to protect against degradation caused by chemical attacks or UV light exposure. It is frequently used for printing driver's licenses, national IDs, and other plastic cards that feature a photo of the cardholder.

Advantages: The process delivers continuous-tone colors with exceptional consistency and quality through precise control of heat. D2T2 is frequently used for government-issued identity documents because an extensive color range allows for brilliant, life-like images. A wide range of desktop and central issuance card printers use this technology.

Direct pigment thermal transfer printing

Monochrome images can be printed on cards using standard graphics thermal printing technology (i.e., ribbons and printheads). The technology does not contribute heavily to document security, but it does allow for fast, low-cost printing of text and images. Direct pigment thermal transfer printing is often used for machine-readable systems.

Applications: This technology is usually used in combination with color printing applications when printing biographical data and for bar codes and OCR machine readable applications.

Advantages: This printing process is fast, highly economical and often quite durable. Because it's a common technology, printers and supplies are easy to find.

Retransfer pigment ink printing

Pigment inks, which are often more stable than dyes and are exceptionally resistant to fading under UV light, can also be applied using the same retransfer technology as dye sublimation retransfer printing. In this process, images are thermally printed to a carrier and are transferred to the substrate. The retransfer process allows for high image quality and makes it easy to accommodate irregularities in the card surface, such as embedded smart card chips and many types of card substrates including polycarbonate cards.

Applications: Government agencies choose this technology for ID cards for its ability to print at 600 dpi and to accommodate smart cards and non-standard composite card substrates, as well as its high resistance to UV fading.

Advantages: Thermally applied pigment inks are more stable than typical dyes and are exceptionally resistant to fading caused by UV light. The imaging process is fast, reliable, and consistent, and when used in conjunction with specialty printheads and unique metallic gold and silver, spot color printing can be enabled.

Drop on demand printing

Drop on demand (DoD) technology uses multiple pressurized printheads to direct fine drops of ink specifically where required. The ink cures quickly using a UV-curing light for durability. DoD varnish can be added to protect the primary portrait or to create additional security features, extending the document life to 10 years.

Applications: Ideal for passports, national IDs, government employee badges, driver's licenses, and other documents with secure color photo requirements.

Advantages: This technology UV-cures the ink, which results in durable color personalization for high-quality, full-color portraits and other personalization elements. DoD images can be registered to laser engraving for a long-lasting, secure color document.

Aqueous Inkjet printing for passports

Inkjet printing technology delivers crisp imagery in a fast and affordable process. Advances in inkjet technology have improved the quality, durability, throughput, and cost over the previously popular toner-based electro-photographic systems.

Applications: The technology is commonly used for low volume passport personalization

Advantages: Key benefits of aqueous inkjet printing include low costs per passport and low capital investment in printing equipment. High-quality photos and biographical data permeate into the paper. Tamper resistance is added to the passport data page by applying a thin film security overlay.

COLOR PLUS LASER SECURITY FEATURE COMBINATIONS

Printing a color photo directly over an engraved image creates a stronger security feature. The laser image that is registered under the color image is permanently engraved and cannot be easily removed without damaging the credential. In addition, the laser image is easily seen under infrared lighting. This results in images that are difficult to remove, alter, or replicate. Entrust supports three color technologies that work well with laser to create secure color plus laser solutions. Combine one of these high-resolution color technologies with the laser photo to provide trusted, secure, tamper evidence.

D2T2 Color Plus Laser

Combine high-resolution dye color and laser photo to provide tamper evidence. Used in conjuncture with biographical data laser engraved into the polycarbonate card helps enable secure personalization that cannot easily be altered.

Drop on Demand Plus Laser

Using UV-curable ink combined with laser engraved photo provides tamper evidence. This vibrant, durable color solution, along with the additional laser engraved biographical data helps enable a secure, long-life color card.

Retransfer Color Plus Laser

Print the image with the Datacard® Artista® VHD Retransfer Printing Module Gen 2 to provide high-resolution pigment color and edge-to-edge personalization. Pigment printing has a higher resistance to UV fading and works well when personalizing non-flat cards or unique substrates. Combined with laser engraving, this solution provides the security required in the market.

LASER ENGRAVING

Laser engraving photos, text, and other graphic elements is considered a secure and durable personalization process. Polycarbonate substrate molecules are hit by a focused laser beam and converted to small, black carbon bubbles that combine to form visible marks on the document, such as text and images. Varying the amount of laser energy enables true grayscale printing for photo-quality monochrome images. The result is difficult to alter or remove.

Applications: High security, consistent image quality, and high durability make laser engraving a core technology for passports, national IDs, government employee badges, driver's licenses, and other documents with high security requirements.

Advantages: The process is reliable and uses no print ribbons or overlays. Because images and text are created below the surface of a document, they are exceptionally hard to replicate, remove, or alter. In addition, many security elements can be achieved, such as tactile engraving, tilted laser imaging, laser ablation, and microprint.

TACTILE CHARACTERS

Embossed and braille characters

Individual characters are "stamped" into the back of the card and are visible on the front as raised characters. Embossing technology can also be used to add braille characters to plastic cards. This provides an effective Level 1 tactile security feature.

Applications: Although flat card technology is increasing in popularity, embossing is still a core technology for financial cards and other applications where a card imprint is required. Some identification card programs use embossed characters to add unique tactile codes.

Advantages: Embossed characters cannot be easily removed or altered without clear, visible detection.

Secure indent printing

Variable indenting creates a recess in size I and size IV character fonts as well as unique symbols on any area on the front or back of the card. Options also include patterned and outline indenting that provide unique marks and impressions within the alpha numeric characters.

Applications: Documents that require visual identity verification can use secure indent printing to protect images from being altered, forged, or removed. Tampering attempts are highly evident.

Advantages: This is a simple and cost-effective solution for adding a Level 1 security feature to identification cards. No special devices are required for inspection by field personnel. Variable indenting is difficult to remove and offers tactile verification. Fraudulent photos cannot be printed over indented characters without creating visible evidence of alteration.

Tactile impressor

The tactile impression feature uses heat and pressure to produce a static, generic, or custom impression on the applied laminated and card substrate. The impression visibly alters the card and laminate and will display tamper evidence if removal of the patch is attempted.

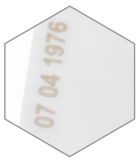
Applications: Documents that require visual identity verification can use a secure tactile impression to protect images from being altered, forged, or removed. Tampering attempts are highly evident.

Advantages: This is a simple and cost-effective solution for adding a Level 1 security feature to identification cards. No special devices are required for inspection by field personnel. The feature can also be used to add additional branding with iconic images such as the Canadian maple leaf or a state seal.

Personalization Security Features

TACTILE LASER ENGRAVING

Laser engraving can be applied in a manner that disturbs the document's surface, creating a tactile effect. This widely used feature serves as a subtle element that can be easily verified by document users or field inspectors. Because it is created using laser technology, it is difficult to alter.



LASERTACT™ SECURITY FEATURE

Unlike ordinary tactile laser engraving, this process creates a wider and a more pronounced raised effect that works well for key biographical information such as the date of birth. The feature is very durable and difficult to remove or alter. It is meant for use on polycarbonate cards or passport substrates.

PERSOCURVE™ SECURITY FEATURE

The PersoCurve™ feature uses biographical information such as the surname, given name, and/or date of birth to form a curved graphic element that is then personalized on the document. The graphic typically varies the font size throughout the element, making it difficult to reproduce or counterfeit. PersoCurve can be applied using laser technology.

FORENSIC PERSOCURVE™ SECURITY FEATURE

Forensic PersoCurve™ builds on the security of PersoCurve™ by either warping the arrangement of data or manipulating pixel density in ways that make the printed element even more difficult to counterfeit. By combining dot pitch and laser pixel path variations with normal PersoCurve™, various subtle (but forensically identifiable) changes in appearance and tactility can be achieved within a single engraved element.

FORENSIC LASERSHADOW™ SECURITY FEATURE

Forensic LaserShadow™ is created using laser engraving technology to create a subtle backdrop of variable text or images behind other personalized data fields. This unobtrusive effect provides one way to add an additional portrait to the document. Multiple portraits, all in different technologies, make the document harder to alter or counterfeit.

CHANGEABLE LASER IMAGE OR MULTIPLE LASER IMAGE (CLI/MLI)

Laser engraving can be used to apply multiple overlapping images and text to a card or a passport. By precise registration of the multiple elements, characters and photos are engraved into a lenticular lens that makes them appear to change when tilted and viewed from various angles. This effective Level 1 security feature is readily visible and is difficult to replicate or alter.

MICROPRINT

Laser engraving – or high-definition retransfer printing technology exclusively available on the Datacard® MX6100™ Card Issuance System featuring the Datacard® Artista® Color Printing Module – can be used to print small text that can only be read with the help of a magnification device. To the naked eye, microprint often is overlooked. This is considered a core security feature in a majority of government identity programs, especially for the issuance of passports, national IDs, and driver's licenses. Stronger microprint security features include personalization data.

GHOST IMAGES

A photo-quality grayscale secondary image (usually a portrait) is difficult to replicate and to remove without detection, especially when combined with overlapping text. Forensic LaserShadow™ (described elsewhere) is a form of ghost image, with stronger security characteristics. D2T2, retransfer, and inkjet printing can also be used to create full-color or faded ghost images.

ULTRAVIOLET FLUORESCENT PRINTING

Today, most ultraviolet fluorescent (UVF) printing is static, and is applied during the book or cardstock manufacturing process. Personalized UVF effects such as text or portraits can be applied with ribbon-based or drop on demand printing technology. Adding covert elements with an ink that fluoresces under ultraviolet light is growing in popularity.

PERFORATION FOR PASSPORTS

Laser technology perforates a series of dot matrix characters through the paper pages of the book and back cover. The perforation security feature is a Level 1 feature that can be easily identified and reveals characteristic brown scorch marks not made in mechanically perforated pages. The perforation can be created using shapes or conical holes (dimensions change as the laser drills through the booklet), thus making it difficult to substitute or exchange paper visa pages in the finished book. Laser perfing can be accomplished at time of book manufacture or inline during personalization.

LASER ABLATION

Laser ablation is a subtractive process of removing material from the document using a laser beam. What remains after the ablation is complete is a clear window displaying an image (usually a portrait) with high resolution. This is yet another way additional portraits are used to create a more secure document. It offers a strong defense against counterfeiting, tampering, and photo substitution.

PHOTO OPTIMIZATION

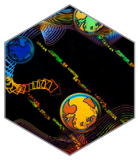
Despite high investments in capture technology and post-capture image manipulation, card and passport issuers often struggle with poor quality photos, which once personalized on the document, detract from its security. A sharper, clearer, more consistent portrait is a better Level 1 security feature and can help intercept imposters who are presenting a stolen document. The Entrust solution dynamically evaluates each image and optimizes certain digital characteristics of the image to optimize it. Useful for portraits and signatures.

LASER SURFACE IMAGING ON POLYCARBONATE

Laser Surface Imaging™ (LSI) is created on a variety of plastic materials including polycarbonate and optical variable devices (OVD) in the substrates by heating the materials with a precisely controlled laser. The laser displaces a small amount of material in a bitmap pattern without carbonizing, vaporizing, ablating, engraving, or removing substrate material.

The desired effect is a personalized image (e.g., photo) or text that is easily seen when viewed under reflective lighting. The process produces a range of effects from nearly undetectable surface ripples to very small bumps, which have different surface reflective properties than the unprocessed area surrounding the personalized image. In addition, LSI can be combined with other technologies such as laser marking and drop on demand printing, to further secure the document. The LSI technology creates a one-of-a-kind substrate for the drop on demand printing layer.

Overlay Material Technologies



POLYESTER LAMINATES

Polyester laminates, such as the Datacard® Duragard® Laminate, provide long-lasting, near-edge protection against abrasion and chemical alteration. They can also incorporate UV blockers to improve fade protection. They are extremely flexible and can significantly extend the useful life of many types of ID documents.

Applications for ID documents typically use laminates ranging from 12.5 microns (0.5 mil) to 25 microns (1.0 mil). Both varieties are available in clear or holographic formats. The latter also can be combined with other OVD security features to further enhance security.

Applications: Polyester laminates are used on a variety of government-issued documents, including national IDs, driver's licenses, entitlement cards, employee badges, and other documents that require both durability and security for a long life in a variety of challenging environments.

Advantages: Polyester laminates help protect many printing technologies from fading and extend the life of documents, which helps minimize costs associated with the replacement or reissuance of damaged cards.

OVER-THE-EDGE OVERLAYS

Government agencies can extend the life and improve the aesthetic value of cards through the application of over-the-edge clear overlays. Products such as the Datacard® DuraShield™ clear overlays are a 7 to 9 micron coating that is applied to a substrate using a heated roller application. The performance of the DuraShield overlay rivals both the exceptional durability of polyester patches and the aesthetic and security appeal of topcoats.

Applications: Over-the-edge overlays are applied like a thin layer topcoat and provide significantly higher resistance to abrasion and chemical attack. While these overlays are new to the market, they have been proven to offer significantly longer card life than standard topcoats. Furthermore, over-the-edge overlays offer stronger adhesion to card substrates, making the document more secure against alteration or counterfeits as the coatings cannot be removed from the substrate intact, or without visual tamper evidence in the case of polyester patch offerings.

Advantages: Performance demonstrated in abrasion and adhesion rivals that of polyester patches commonly used today. Over-the-edge application also greatly enhances the appearance of cards, while adding extra security.

CardGard™ UV-curable topcoats

Ultraviolet-cured topcoats are 5 to 7 microns thick and cannot be removed intact, providing a high level of security. Products such as Datacard® CardGard™ UV-Curing Topcoat offer increased durability compared to standard topcoats.

Applications: CardGard™ topcoat provides a level of protection above standard topcoats by protecting against chemicals, moisture, UV light, and abrasions. Over-the-edge topcoats cannot be removed without evidence of tampering. A UV-curable coating is transferred to the personalized card and transforms into a tough abrasion and chemical-resistant layer after curing with UV light.

Advantages: These easy-to-apply topcoats offer aesthetic value at an affordable price. Government agencies choose UV-cured topcoats to reduce costs when no security features are required.

Thin film topcoats

This is the most economical card protection solution offered by Entrust. This protective coating, typically 2 to 4 microns thick, is applied to personalized cards using a printhead or heated roller. All color printed cards need this added layer of protection to prevent print degradation. Thin film topcoats are available in clear and holographic varieties to meet various security requirements.

Applications: Standard topcoats are commonly used on employee ID cards or other applications in which the card is primarily used for visual identification.

Advantages: Topcoats are designed to prevent dye migration and provide limited abrasion and chemical resistance for cards that do not have long life or high usage requirements.

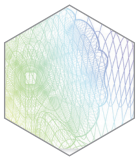
THIN FILM OVERLAYS FOR PASSPORTS

A thin polymer film, which may include registered holograms, microtext, and laser retrievable text, can be quickly and economically applied to passport as part of an inline personalization process. Application of thin film overlays provides government agencies with multiple lines of defense against forgery and alteration. Available in holographic format, it provides durability and a high level of security to the passport against any alteration or counterfeiting. It is typically 8 to 12 microns in thickness and is applied with a heated roller or platen application.

Applications: Unlike plastic cards, passports and other paper-based documents are not exposed to heavy use in swipe readers and rarely come in contact with plasticizers found in wallets. This makes passports a perfect candidate for thin film coatings, such as the Datacard® Optigram® thin film overlay.

Advantages: Thin film overlays with overt and covert security features are highly effective for providing passport security. Level 1, 2 ,and 3 security features are easily and affordably incorporated.

Overlay Security Features



HOLOGRAMS

Holograms, which are composed of two superimposed two-dimensional pictures of the same object seen from different reference points, provide excellent overt security for identity documents. They can be seen by the naked eye, but they cannot be reproduced by conventional printing processes or color copiers. Entrust offers a very large portfolio of high security level 1, 2, and 3 holographic features, originated using multiple technologies and designed for real work verification. Information on this portfolio and on individual security features is available upon request.

Level 1 - Overt

2D hologram
Images, lines, or text that refract light utilizing the full color spectrum. Color changes as viewing angle changes.

Pseudo color
Image will refract its true colors when viewed at a very specific angle.

Grayscale color
Images, lines, or text that has no color refraction but is comprised only of neutral grays, white, or black.

2D/3D or multi-plane hologram
Images, lines, or text that is comprised of elements on the surface, background or above the surface plane. Elements on the background or above the plane exhibit a sense of depth and parallax.

2 channel/flip image
Two distinct images that occupy the same area of the hologram and shift from one image to the other as it is viewed from different angles

Guilloche security patterns
High-resolution lines, curves, rosettes, or a combination of all these elements. Designs are created utilizing highly sophisticated computerized software and each line can be assigned a predetermined color shift to move in synchronized animation.

Embossed effect
Optical illusion of relief created by a highly diffractive surface-oriented grating that can be applied to images, text, or lines in a hologram.

Achromatic effect
Dramatic kinetic black and white image switch.

Kinetic animation effect
Patterns that appear to animate, giving the effect of motion, when rotated.

Stereogram
3D-like effect when viewed, giving the image a perceived “depth” when viewed even though the hologram is all contained in the same place. One image within the hologram appears to float above the other.

White matte text
Non-diffractive text when a white, matte finish.

Line width modulation (also available in Level 2 and 3)
Various image and text effects that can be created by the mathematical manipulation of width, length, and height of lines.

Watermark effect
Unique effect where a translucent relief of an image or text gives the impression of some areas to be convex.

Lens effect
Images appear to be 3-dimensional in body. When viewing with a flashlight, letters or other micro information can be recognized.

Level 2 - Covert

Micro text
Diffractive or non-diffractive text, which size can be as small as 175 micron. Can be deciphered with the use of an eye loop or magnifying glass.

Level 3 - Forensic

Covert laser retrievable image or text (single axis or dual axis)
Images or text completely undecipherable by the human eye and can only be decoded by illuminating the coded area with a laser device and looking for the refracted light as is projected back at a specific angle. CLRs can be dual axial in which a different text or image can be viewed at 90 degrees from each other.

Micro imagery
True color images or photographs that are reduced to a size as small as 3 mm square.

Digital Technologies

SMART CARD TECHNOLOGY

Smart chips can be programmed to store applications, biometric identifiers, and demographic data relating to the cardholder. Biometrics provide inspection officials with the ability to retrieve photos, fingerprints, or other unique identifiers to confirm that document presenters are who they claim to be. Both contact and contactless chips and combined hybrid contact and contactless chips can be encoded as part of the inline personalization process in desktop and high-volume card personalization systems. The ability to store and run applications makes smart cards ideal for electronic payments and a variety of other transactional applications, including transportation, loyalty, healthcare, telecommunications, and membership.

CONTACTLESS CHIPS FOR PASSPORTS

Passport chips are commonly encoded with the citizen's portrait and biographical information using chip encoding software and applications. This information is retrieved when the passport is presented for inspection, to confirm that the document presenter is who they claim to be.

BAR CODES

Bar codes are optical machine-readable elements that provide convenience more than security in processing the document. They may be printed on a card, passport, or other identity document and contain demographics and other kinds of data. One-dimensional (1D) bar codes – constructed with parallel lines of varying widths – hold minimal amounts of data, typically fewer than 100 characters. Two-dimensional (2D) bar codes are comprised of rectangles, dots, hexagons, and other geometric patterns. 2D bar codes can store thousands of characters. Bar codes are often used in read-lookup applications.

MAGNETIC STRIPES

Magnetic stripes can be encoded with biographical and security data for transaction terminals, access control systems, and other similar devices. Government agencies frequently use magnetic stripes on driver's licenses, entitlement program IDs, and other applications that involve swipe readers or point-of-sale terminals.

Technology-Printer Matrix

Entrust issuance systems produce documents that contain your choice of technologies and security features.

	Desktop Card Printers			Central Issuance Card Personalization				Central Issuance Passport Personalization		Distributed Issuance
	Sigma DS3 w/CLM	Artista CR805 w/CLM	CL900	MX1100™ MX2100™	MX6100™	MX8100™	MX9100™	PB8500™	PB6500™ Compact	PB1000™
PERSONALIZATION TECHNOLOGIES										
Printing										
Direct dye sublimination printing	•									
Direct pigment thermal transfer printing				•	•	•	•			
Retransfer pigment ink printing		•			•					
Drop on demand (DoD) printing					•	•	•	•		
Aqueous Inkjet printing for passports									•	
Laser			•	•	•	•	•	•	•	•
Tactile Characters										
Embossed and braille characters				•	•	•	•			
Secure indent printing				•	•	•	•			
Tactile Impression	•	•								
SECURITY FEATURES USING PERSONALIZATION TECHNOLOGIES										
Tactile laser engraving			•	•	•	•	•	•	•	•
LaserTact™ Security Feature			•	•	•	•	•	•	•	•
PersoCurve™ Security Feature			•	•	•	•	•	•	•	•
Forensic PersoCurve™ Security Feature			•	•	•	•	•	•	•	•
Forensic LaserShadow™ Security Feature				•	•	•	•	•	•	•
CLI			•	•	•	•	•	•	•	•
MLI				•	•	•	•	•	•	•
3D photo			•	•	•	•	•	•	•	•
Microprinting			•	•	•	•	•	•	•	•
D2T2 color plus laser				•	•	•				
Retransfer color plus laser		•			•					
Drop on demand color plus laser					•	•	•	•		
Ghost images	•	•	•	•	•	•	•	•	•	•
Variable ultraviolet printing					•					
Perforation for passports								•	•	
Photo optimization			•	•	•	•	•	•	•	•
LSI™				•	•	•	•	•	•	
OVERLAY MATERIAL TECHNOLOGIES										
Polyester laminates 1 mil	•	•		•	•	•	•			
Polyester laminates 1/2 mil	•									
Over-the-edge overlays (Durashield)	•									
CardGard ultraviolet-cured topcoats				MX2100 only	•	•				
Thin film topcoats	•			•	•	•	•			
Thin film overlays for passports								•	•	
SECURITY FEATURES IN OVERLAY MATERIALS										
Holograms – Level 1, 2, and 3	•	•		•	•	•	•	•	•	
Security printing	•	•		•	•	•	•	•	•	
MACHINE-READABLE TECHNOLOGIES										
Contact/contactless smart chips	•	•	•	•	•	•	•	•	•	•
Bar codes	•	•	•	•	•	•	•	•	•	•
Optical character recognition (OCR)	•	•	•	•	•	•	•	•	•	•
Magnetic stripes	•	•	•	•	•	•	•			

Glossary of Terms

AAMVA – American Association of Motor Vehicle Administrators.

ANSI – American National Standards Institute.

Anti-Copy Pattern – A security print design that fools or confuses a scanner into producing an inaccurate copy of the original.

Biometric – A measurement of a person's physical or behavioral characteristic, to aid identification and/or verification.

Centralized Issuance – The issuance of documents from a single physical site as opposed to many decentralized sites.

CLI – Changeable laser images; multiple images that occupy the same space, formed by engraving through a lens structure. Commonly used on cards.

CMYK Process – Uses four colors (cyan, magenta, yellow, and black) to give the illusion of a wider range (gamut) of colors.

Composite Card – A card manufactured using layers of different polymer in an attempt to combine the best properties of each.

Contact Chip – An integrated circuit (IC) that requires contact, through a contact plate, to exchange data with a reader or writer.

Contactless Chip – An integrated circuit (IC) that allows for storage of biographical data and biometrics and can be read with a reader at close proximity.

Dual-Interface Card – A card with both contact and contactless interfaces. With such a card, it becomes possible to access the same chip via a contact or contactless interface, with a very high level of security.

Counterfeit Document – An unauthorized document that has been created to look and perform like a genuine ID (card or passport), usually using illegal fraudulent techniques. Counterfeiters make copies from substitute materials that resemble the materials that are used for the genuine documents for the purpose of escaping detection.

Dye Diffusion Thermal Transfer – A digital print process (D2T2 or "dye sub") that uses three or four color ribbons containing dyes.

Digital Printing – Printing data from a computer file rather than a physical plate, allowing variability for images and personalization.

Dithering – The use of patterns of dots in digital printing to give the illusion of a wider range (gamut) of colors.

DOVID – Diffractive Optically Variable Image Device, commonly called a hologram; a Level 1 anti-copy security device.

Duplex – Two-sided, either two registered security print workings, or a printing machine that can print on both sides.

Guilloche – A printed security pattern with intricate, repetitive elements. Once difficult to counterfeit, less effective now.

Halftone – The use of dots of varying size in commercial printing to give the illusion of varying density.

Hologram – Originally a 3D image, is now the common name for a diffractive optically variable image device (DOVID).

HRI – High refractive index; material that is used to enable a transparent DOVID to be both reflective and transmitting.

IC – Integrated circuit; "chips" in a smart card or passport that may be a smart microprocessor or dumb memory.

ICAO – International Civil Aviation Organization.

ID-1 Size – Accepted international standard (in ISO 7810) for ID card dimensions: 85.60 mm × 53.98 mm (3.370 in. × 2.125 in.).

ID-3 Size – Accepted international standard (in ISO 7810) for passport dimensions 125 mm × 88 mm (4.921 in. × 3.465 in.).

Impersonator – A person who attempts to look like the photograph in an ID document that is not rightfully theirs.

Impostor – A person who fakes entitlement to an ID document before it is issued.

Intaglio – A specialized security print process, forcing thick paste ink from a recessed engraved plate to produce tactile print.

ISO – International Organization for Standardization.

Kinegram – Specialized proprietary diffractive optically variable image devices (OVIDs) from the Swiss company OVD Kinegram, a member of the German Kurz group.

Laminate – The protective layers on the outside of a card, or a single layer within a multi-layer construction.

Lamination – The process of sticking layers together. Needs a thermal adhesive or uses the natural properties of the polymer.

Laser Engraving – A digital imaging process where lasers are used to engrave or mark a suitable substrate.

Letterpress – A process that prints text from moveable type, often used to print sequential document numbers.

Level 1 Security Feature – An overt feature that requires no device and little or no training to use.

Level 2 Security Feature – A covert feature that requires a device and some knowledge or training to use.

Level 3 Security Feature – A deeply hidden, forensic feature that requires knowledge, expertise, and equipment to use.

Lithography – Often referred to as “litho”; a printing process that is common in both commercial and security printing.

Microprinting – Tiny printed text, barely discernable with the naked eye. Digital processes cannot easily resolve it.

MLI – Multiple laser image; multiple images that occupy the same space and are formed by engraving through a lens structure. Commonly used with passports and cards.

NCITS – National Committee for Information Technology Standards.

OCR – Optical character recognition; a system whereby special fonts are used to enable machine reading of text.

Offset Litho – A variation of litho printing when an image is first printed onto a rubber blanket before being offset to the substrate.

OVD – Optically variable device; includes DOVIDs and printed OVDs such as OVI and iridescence.

OVI – Optically variable ink; a proprietary feature from the Swiss ink maker SICPA, that changes color at different angles.

Optical Memory Card – A proprietary (Lasercard) high-capacity system of data storage using optical storage.

Personalization – The transfer of personal biographical data onto the ID document using technology such as laser or printing.

PET – Polyethylene terephthalate, or “polyester”; a polymer used in ID card construction. May be glycol modified (PETG).

Photo substitution – The primary attack of documents using applied photographs, where the genuine photo is replaced.

Pigment – A colored material that tends to be insoluble in its vehicle (dyes are soluble), and often more durable than a dye.

PIN – Personal identification number.

Polycarbonate – Sometimes referred to as PC; a tough durable polymer used for ID cards and passport data pages.

PVC – Polyvinyl chloride; a plastic material used as the substrate in many financial cards and low-cost ID cards.

Rainbow Printing – A security print technique whereby different colored inks are merged to produce anti-copy effects.

Retransfer – A digital printing refinement where the image is first printed to a carrier material before being re-transferred.

Silk Screen – Also known as “screen”; a printing process whereby ink is forced through holes in an imaged stencil. Often used for OVI.

Security Printing – A specialized form of printing used to defend documents of value against counterfeiting and forgery.

Substrate – The base material from which a document is made and to which print is applied. A blank card or passport that has yet to be personalized.

Tactile Feature – A security feature that can be felt because it is either raised above or recessed below the surface.

Taggant – Any detectable material, often proprietary, included secretly within a document, often in very small (trace) amounts.

Template – A compressed data file of biometric characteristics; used in many biometric systems to reduce file sizes.

Teslin – A proprietary plastic substrate made by PPG. A common ID card substrate, protected by polyester laminate.

Topcoat – A 2 to 3 micron thick protective film on the outer surfaces of a card. Cannot be removed intact, thus tamper evident

UV Fluorescence – A glow produced when special ink is illuminated by ultraviolet light. A common Level 2 security feature.

Web Printing – A continuous roll of paper or plastic substrate. Contrast with sheets.

A commitment to relentless innovation

The world changes rapidly. Populations increase, global markets emerge, and security threats become smarter and more dangerous. We understand the challenges facing government agencies and we are committed to the relentless development of new technologies to address those challenges. Entrust's comprehensive portfolio of end-to-end government solutions bridges the gap between physical and digital security, offering solutions to create and verify trusted identities – all with the most advanced technology.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223