ITW Security Division

Secure Personalization – It's Not Just Black and White

An ITW Security Division White Paper – December 2016

COVID
ITW Security Division

Fasver
ITW Security Division

Imagedata
ITW Security Division

Overview

"The rapid growth in identity fraud has led to increasing concerns over the security of Driving Licence (DL) and ID cards and many other types of documents used to confirm identity. DL/ID cards are often accepted not only as proof of having earned the privilege to drive a motor vehicle, but also as confirmation of the identity of the holder for obtaining access to a wide variety of other services, for example opening bank accounts, withdrawing or transferring funds etc.

Of particular concern is the opportunity DL/ID cards have to serve as evidence of identity to assist in building a false identity and providing a pathway to obtain other documents, such as passports, all in an assumed identity. For these reasons DL/ID is a target for the fraudster making it important to ensure that DL/IDs are adequately protected from the various forms of fraud to which they may be subject."
(AMVAA DL/ID Card Design Standard, August 2013)

The need for highly secure personalized documentation has never been greater – with increasing levels of people movement and heightened threats – identification document issuers are always looking for improved methods to secure and authenticate a travel or personal identification document.

An essential aspect of securing an identification document is ensuring that the document is linked to the true identity of the document holder, via secure personalization. Due to the personal data being most at risk of fraudulent alteration, personalized security features are now a highly desirable attribute in security document production today.

This paper looks at some of the techniques available to help prevent portrait alteration and provide secure personalization, in particular highlighting new techniques that are difficult to either copy or simulate by counterfeiters.

Security Personalization

Document personalization is defined as:

"the process by which the portrait, signature and/or other biographical data relating to the holder of the document are applied to the travel document. These data record the personalized details of the holder and are at the greatest risk of counterfeit or fraudulent alteration. One of the most frequent types of document fraud involves the removal of the portrait image from a stolen or illegally obtained travel document and its replacement with the portrait of a different person"
(ICAO 9303 MRTD 7th Ed. 2017_pt2)

Photographs included on ID cards and documents using non-secure personalization techniques, such as ink-jet or standard D2T2 printing, can be a target for substitution and therefore anti-counterfeiting efforts often concentrate on tamper prevention and tamper evidence. This makes the image of the ID document holder a real focus for counterfeiters, to the extent that ***"Plastic cards are the product most targeted by fraudsters"*** (Gary Mile, UK's Metropolitan Police, FALCON, SDW 2015).

The complexity of ID cards is therefore an essential consideration when looking at their overall security. Protection from counterfeiting or photographic alteration activity can be increased with the addition of a secondary personalized image to an ID document, particularly if that secondary image is made with a technique not easily accessible to the fraudster. So whilst two ink-jet images may double the work for the counterfeiter to alter the images on the ID, if that technique is readily available to the fraudster, then once the document has been effectively tampered with, photo substitution will simply occur for both images. However if the secondary image is produced with a secure personalization technique, this adds much more complexity to any fraudulent attempt to alter the personalised data and so becomes a key part of securing an ID card or document.

In addition to varying the imaging techniques, it is also important to consider when security features are added to cards in the production process. Those added at the point of issuance are highly effective as they allow the security document manufacturer to provide the final level of security at the very end of the ID document's production. This also ensures that any consumables such as the card or ID document blanks yet to be printed, become much less valuable to

fraudsters, as the important security is yet to be applied to them and also removes risk of fraudsters access blank documents during production, transportation and storage.

Overall security can be further enhanced by making the security feature individual to each document and even more so if this individualization can be personalized to the specific holder of the final ID document. Therefore, restricted consumables for personalization at point of issuance that cannot be easily mimicked by other techniques are also highly desirable.

New ID substrates

Over the past 10 years the security document industry has seen changes in document substrates, which have driven a change in photo personalisation techniques, to the extent that almost three quarters of passports issued between 2006-2016 were personalized with either ink-jet or laser engraving[1].

Ink-jet printing, whilst a common method for adding colour photographs to ID documents, is also widely commercially available and as such can be easily replicated by a fraudster. Therefore, the security of any ink-jet personalized document must come from other techniques and features added, alongside the need for highly robust tamper-proof protection of the personalized data.

Laser engraving, is increasing in popularity as a personalization technique alongside the use of polycarbonate (PC) as a document substrate, however, due to the commercial availability of lasers it is now also possible to directly replicate or alter laser engraved images.

Therefore, complimentary secure personalization techniques are not only needed, they are essential to a secure ID document solution.

Optically Variable Features

A common Level 1 security feature used in many documents today is an optically variable device i.e. a feature that changes in its appearance upon movement of the document.

"where a travel document is constructed entirely of plastic, optically variable security features shall be employed which give a changing appearance with angle of viewing. Such devices may take the form of latent images, lenticular features, colour-shifting ink or diffractive optically variable image features"
(ICAO 9303 MRTD 7th Ed. 2017_pt2)

Examples of such security features include holography and optically variable colour shift pigments. These excellent security features can either be incorporated into the body of a document or on top of the finished article, as a holographic patch for example.

Optically variable pigments can be used during the manufacture of the document[2] or they can be used to make a personalized security feature by utilising these pigments within a thermal transfer type ribbon[3], as shown in figure 1 below.

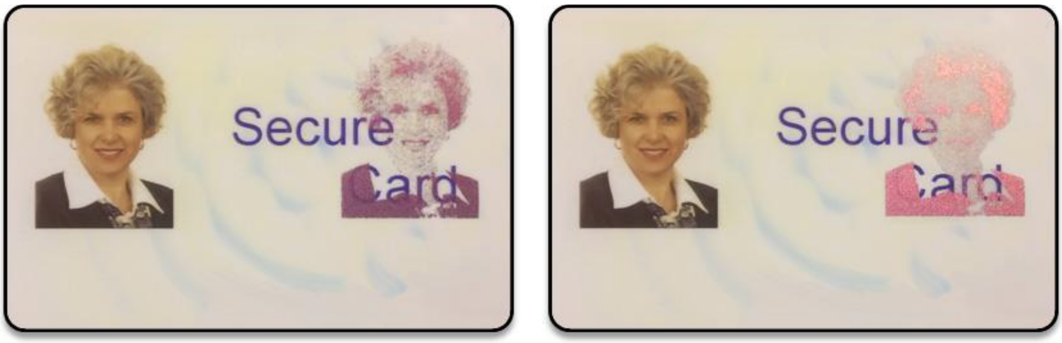

Figure 1: Optically variable personalization from a thermal transfer ribbon

Although the use of optically variable pigments within a thermal transfer ribbon will provide the highly desired end effect of a personalized optically variable feature, the pigments themselves tend to be very expensive, thereby rendering their use on a thermal ribbon very expensive, especially as this is a printing technique with inherent waste. However, optically variable personalized features are not limited to the use of the optically variable pigments themselves. The idea of personalized optically variable features can be taken further than simple use of optically variable pigments. ITW Security Division has unique technology that allows for novel, coloured images with optically variable effects to be created both in and on PC and PVC security cards and documents.

As an example, the image shown in figure 2 below demonstrates a simple effect whereby the personalized face image is either in front of or behind the personalized lettering, depending on the angle of view.

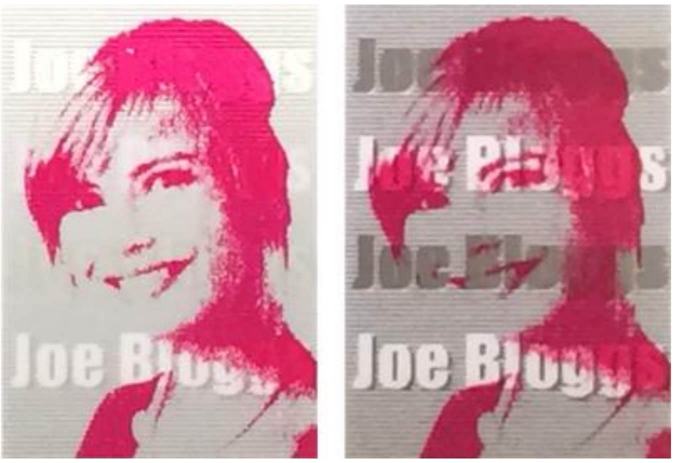

Figure 2: ITW Security Division's unique personalized optically variable effect varies according to the angle of view

Ultra Violet (UV)

A common security feature used in the market today is Ultra Violet (UV), namely a feature or images that are essentially invisible under normal light but show a highly coloured image under ultra violet light. Standard readers deployed at borders usually have hardware sensors with visible, UV-A and IR illumination[4].

Security features fluorescent under UV-A light are available in a range of colours and offer a secure and easily identifiable feature within security cards and documents. A range of colours are already available in the market, with blue UV-A being one of the most prevalent and hence one of the least secure.

Therefore, non-blue UV-A features are more desirable and an example of a yellow UV-A personalized image printed with a transfer ribbon in combination with Dye diffusion thermal transfer (D2T2) printing on a PVC card is shown below in figure 3 and an example of the use of the same yellow UV ribbon in combination with Unichroma + D2T2 printing (see Polycarbonate section below) on to a PC card is shown in figure 4.

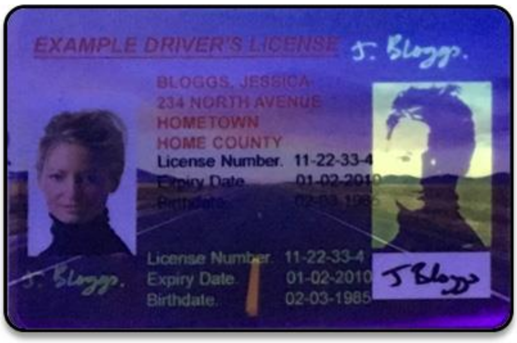

Figure 3: Personalized UV print on a PVC card

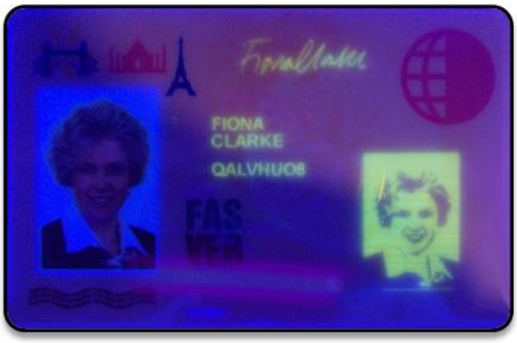

Figure 4: Personalized UV print on a PC card with Unichroma

Personalized UV Features

Many UV-A security features in the market today are not point of issuance personalized features. They are instead features that are incorporated into the document during manufacture i.e. they are pre-designed and are not personalised or in any way altered at the point of issuance. This can be advantageous when imaging something such as the flag of a country, in which case, a non-standard colour or position could alert someone to a fraudulent document. This type of document body security feature can be further enhanced when full colour UV-A image designs are utilized within the document body such as with ITW Security Division's patented[5] Imaprotek technology.

When UV-A features are incorporated in to the body of a document during manufacture this provides excellent durability, image quality and tamper resistance, however, there is no match between the security feature and the information relating to the individual document holder.

Some personalisation printing techniques today already use UV-A security inks to add personalized UV features to cards and documents. For example, security features and secondary images in non-blue individual colours and even full colour images can be added to passport documents using ink-jet printing[6]. However, ink jet printing is currently most suitable for paper documents and is not widely used in the ID card market, where PVC and PC are the substrates of choice.

It is also possible to add single and full-colour UV-A images to plastic cards via mass transfer or diffusion printing techniques such as those used in photographic printing. This technique utilises red, green and blue UVA fluorescent dyes to create a full-colour, photographic quality image[7] that is invisible under normal light but clearly visible under UV-A light. An example is shown below.

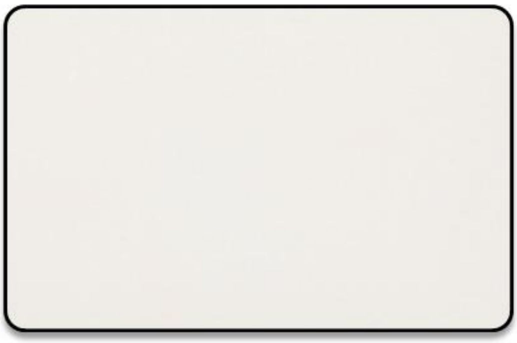

Figure 5: Card in normal light

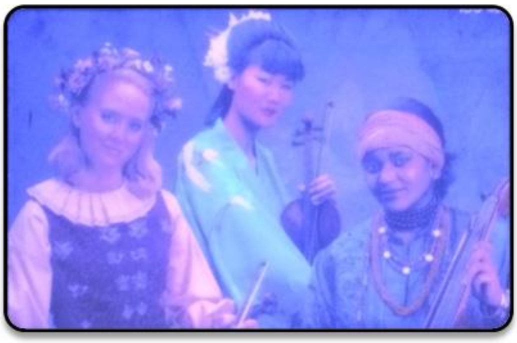

Figure 6: Card under UV-A light with full colour image

Meeting Polycarbonate ID Document Needs

The growth in Polycarbonate (PC) use for ID documents has meant a concomitant trend towards there being no upper-layer protection, such as through a laminate or overlay and used as standard in paper and PVC card ID documents. As security to protect the personal data is mainly applied within these laminates and overlays, PC requires a different approach and there have been a number of developments in the techniques used to integrate security features into the PC document, specifically via the use of lasers. For example variable tactile characters and covert laser images can be added to a PC ID document and registered with the holder's colour photo to build in security[8]. However, whilst these add a level of security to the document, when compared to traditional Level 1 security features, there are still limited options for direct security features from laser engraving techniques.

The market trend has therefore been instead to rely on security features within the PC document body. As an example, holographic features can be incorporated in to the body of a PC document (see figure 7) and this type of feature is in wide use in a number of high profile ID documents today.

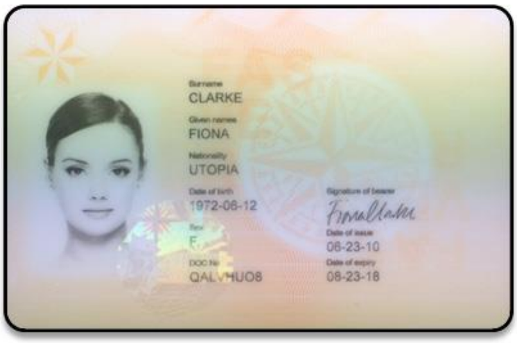

Figure 7: Security built in to the PC document

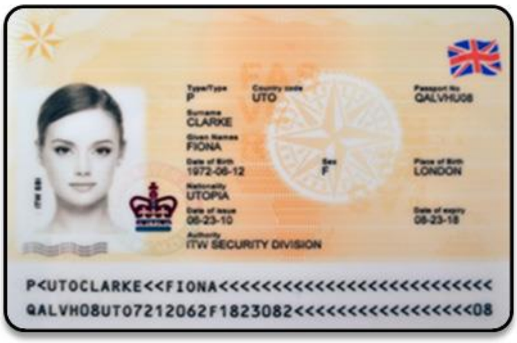

Figure 8: PC Protek™ incorporates security into PC

Further security within the body of a PC card or document can also be achieved through the use of ITW Security Division's new innovation of PC Protek™ - enabling highly secure printed features to be incorporated into the body of a PC document. Figure 8 shows how PC Protek™ features such as metallic, OVTek™ and thermochromic can all be incorporated into a PC datapage. OVTek™ and thermochromic features not only offer a secure level 1 feature but they

are also laser transparent, enabling the full use of laser engraving to personalize and secure the document during its manufacture.

Despite the developments in PC document body security as well as print, holographic and laser security features, there is still a need in the market place for features that can be added at the point of issuance and, more specifically, as part of the personalization step to link the document holder with the point of issuance security feature.

Fraudsters have already shown many different techniques to alter personal data on PC documents. From back-side grinding, laminating of printed thin films on the top surface, milling and filling, and laser re-imaging[9] – all these methods can be used to alter personal data on PC documents. As an approach to make the document more complex the addition of coloured images, secondary images and security images are an obvious way to hinder these current alteration techniques and make the overall document more secure.

Colour images

Colour laser marking is now possible and one method to enable this is to seal photosensitive pigments inside the polycarbonate body during the card manufacture. Precise laser light irradiation is then used to bleach the pigment and allows for the creation of a colour image[10]. Whilst this provides good durability and colour personalisation inside the card body, the image quality is much reduced when compared to standard colour printing due to the reduced sharpness, contrast and colour saturation[10].

An alternative method of adding a high quality colour image to PC cards and documents to improve their security is via the use of ITW Security Division's patented Unichroma^{TM} technology[11]. D2T2 colour printing is a well-known technique in the ID card market today but has been limited to only a few viable card substrates, the most common of which is PVC. D2T2 direct printing does not work on standard PC substrates as it causes either ribbon sticking issues or very poor image quality. ITW Security Division's Unichroma^{TM} removes all these issues thus opening up PC as a viable substrate for direct D2T2 printing.

With D2T2 being a widely available printing technique in the market today the question that may well be asked is: *"Why can this be regarded as an advantage for increased ID document security?"* The answer is simple – Unichroma^{TM} can be printed to directly match the colour photograph size, shape and location of the holder's image on the card. The rest of the card surface therefore remains non-printable with D2T2 card printers. Therefore if the image is removed and fraudulent attempts are made to replace it, without the Unichroma^{TM} technology at the point of issuance, the fraudster cannot use D2T2 to print a new colour image on to the ID.

Below Figure 9 shows a typical D2T2 printed card whilst figure 10 shows the failure that occurs when direct D2T2 printing is attempted on a standard PC card surface. The solution is provided by ITW Security Division's Unichroma^{TM} technology together with direct D2T2 printing on to a standard PC card and can be seen in figure 11.

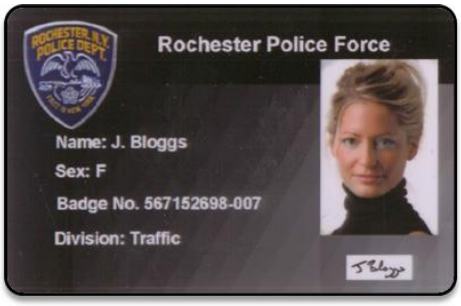

Figure 9: D2T2 Printed PVC card

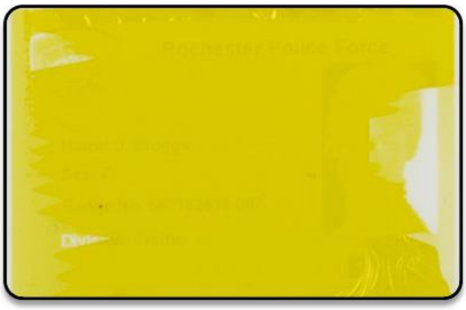

Figure 10: D2T2 Printed PC card

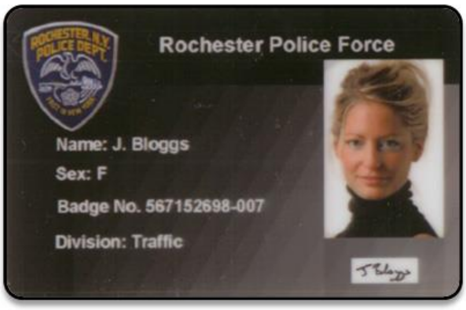

Figure 11: D2T2 and Unichroma^{TM} Printed PC card

UnichromaTM + D2T2 printing is also an opportunity to add a colour photo as a secondary or primary image respectively on to PC cards alongside the other security features.

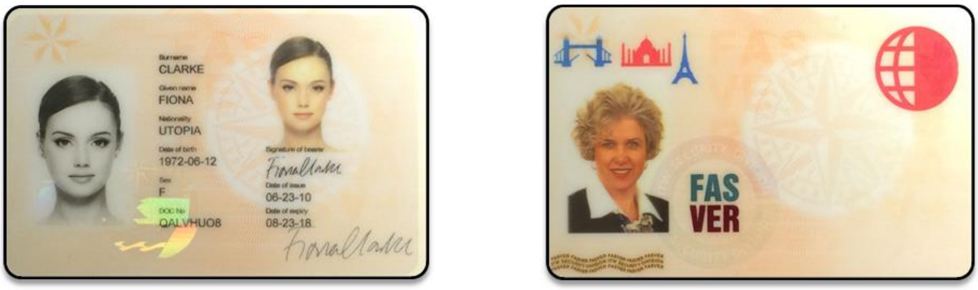

Figure 12: Unichroma^{TM} and D2T2 Printed PC ID documents

Due to the continuous tone nature of an image printed with the D2T2 technique it can be easily identified with close inspection against other dithered image printing techniques such as ink-jet or mass transfer printing. Therefore, even if the fraudster removed the Unichroma$^{\text{TM}}$ and attempted to add an alternative colour image with a more readily accessible printing technique appropriate for PC, this tampering would be identifiable upon close visual inspection.

Secondary portrait image is listed as an ICAO9303 additional feature for protection against photo substitution and repeating of personal data is becoming increasingly popular. Unichroma$^{\text{TM}}$ allows colour imaging via a technique different to that used for the standard monochrome engraved images, it can be used in such a way as to restrict image alteration and can be utilised to enable tamper evidence.

Thus, Unichroma$^{\text{TM}}$ is an ideal complimentary technology to laser engraving for use with PC to add a secondary colour image.

"Even if a security feature appears to be very difficult to reproduce or to falsify, there can be no guarantee it will not become compromised during the validity period of the document. If this happens the security of a DL/ID may be significantly damaged resulting in serious consequences. The preferred approach is to select a set of security features that work together in combination, such that even if one feature becomes compromised the others will continue to provide protection. For the fraudster, having to overcome multiple security features has an important deterrent effect, significantly increasing the time, cost and the risk of detection in perpetrating the fraud and probably turning him to other easier targets."
(AMVAA DL/ID Card Design Standard, August 2013)

Secondary image addition using lasers and "non-standard" substrates can be more than just attempting to replicate colour photographs. For example, standard lasers can be used to engrave images in to metallic areas that have been previously added to the substrate of choice in a select area e.g. by screen printing. The image formed within the metallic area creates an optical effect whereby the image can look positive or negative depending on the angle of view. Figure 13 shows an example of such an image produced by ITW Security Division.

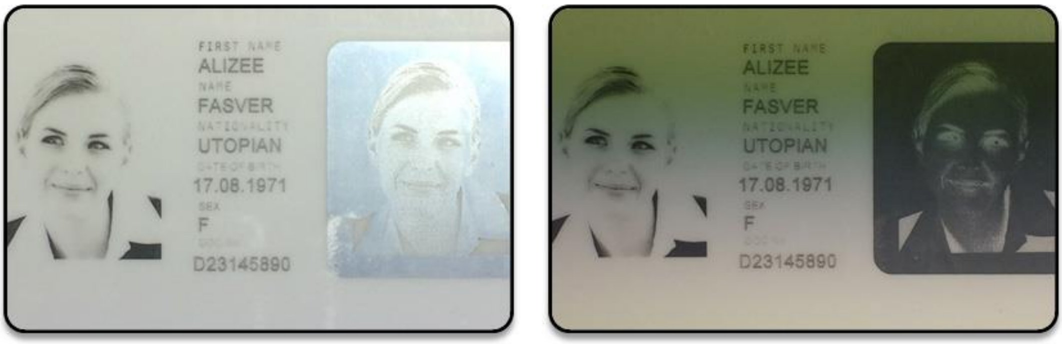

Figure 13

Combining the security industry leading knowledge of Covid, the patented printed features of Fasver with the personalization expertise of Imagedata – ITW Security Division is ideally placed to offer, design and develop novel personalized point of issuance security features to meet the ever-increasing needs of the security document issuer today and tomorrow.

The addition of secondary photographs and personal data to PC cards and documents is no longer just black and white!

[1] Trends in Basic and Additional Security Features; SDW 2016 Conference Presentation; Keesing ID Academy

[2] US2011/0226147

[3] EP1390211

[4] ICAO 9303 MRTD 7th Ed. 2017_pt2

[5] US6494490

[6] http://www.diletta.com/EN/sample_passports.ht

[7] US7286150 / EP1485258

[8] Empowering Security at time of Personalization; SDW 2016 Conference Presentation; Entrust Datacard

[9] Windows in PC Documents: futile or not? SDW 2016 Conference Presentation; Arjo systems

[10] The Price of Colour; SDW 2015 Conference Presentation; Safran Morpho

[11] EP2250030

About Us – ITW Security Division

The ITW Security Division was formed in 2012 through the coming together of the management teams, technologies and resources of Covid®, Fasver® and Imagedata™. Leveraging the strengths of these brands, the ITW Security Division today offers the secure document market a single source supply for high security laminate documents and dye diffusion (D2T2) ribbons.

As an independently operated division of Illinois Tool Works Inc. (ITW), a Fortune 200 company, we have the financial resources necessary to continually invest in new technology, research and development. This global footprint and view has enabled us to supply products to more than half the world's countries from our secure facilities in the UK, France and USA.

At ITW Security Division we understand that the foundation for secure materials begins with highly secure manufacturing facilities. We manufacture products from start to finish in one of our secure facilities enabling us to meet the 'under-one-roof' production requirements demanded by many governments. Our products and technologies driven by our Covid® and Fasver® brands have developed a global reputation for highly advanced security solutions. Overt, covert and forensic security technologies are customised to the specific requirements of each document program to enable the widest combination of personalisation methods and substrates for passport and ID Card issuance worldwide. The companies within the security division include:

ITW Covid Security Group Inc was one of the world's first holographic and OVD manufacturers and now has over 25 years' experience. Located in New Jersey USA, the company is ISO14298 & NASPO (North American Security Products Organisation) accredited and manufactures all of its products under one roof, from holographic design and origination through to shim production, embossing, metallising, laminating, die cutting, converting and packing.

ITW Imagedata is a global manufacturer of consumables for the Card industry located in the UK, specialising in the design and manufacture of D2T2 (dye sublimation) ribbons that we supply exclusively to OEM Card printers. The company is ISO 9001 and ISO 14001 certified.

Fasver® S.A.S.U. is a global leader in the design and production of security products for the protection of personal data on identity documents including Passports & ID Cards. Located in Montpellier, France, the company is ISO & Intergraf accredited and their unique authentication solutions have been protecting documents for over 25 years.

ITW
Security Division

www.itwsecuritydivision.com

Protection for your documents and your business
Covid • Fasver • Imagedata

For more information:
Government Programs - government@itwsecuritydivision.com
Secure Documents - security@itwsecuritydivision.com