ITW Security Division

The Physical ID Card is Dead – Long live the Physical ID!

An ITW Security Division White Paper

COVID
ITW Security Division

Fasver
ITW Security Division

Imagedata
ITW Security Division

Overview

We live in a world which is continuing its rapid growth towards mobile and digital formats for a wide variety of everyday tasks. Convenience and ease of use are key drivers, together with the growth in smart phones, meaning that many are now looking for their identity documents such as national IDs and driver licenses to ultimately follow the trend towards digitalisation and mobility.

This growth has led to the creation of Digital IDs and the capability to use our smart phones to carry a traditional physical ID card via a secure, digital credential – called a Mobile ID.

So, with the growth in smart phones and this new capability for Mobile ID, does this mean that physical ID cards are no longer needed?

An example of a physical ID cards with integrated security

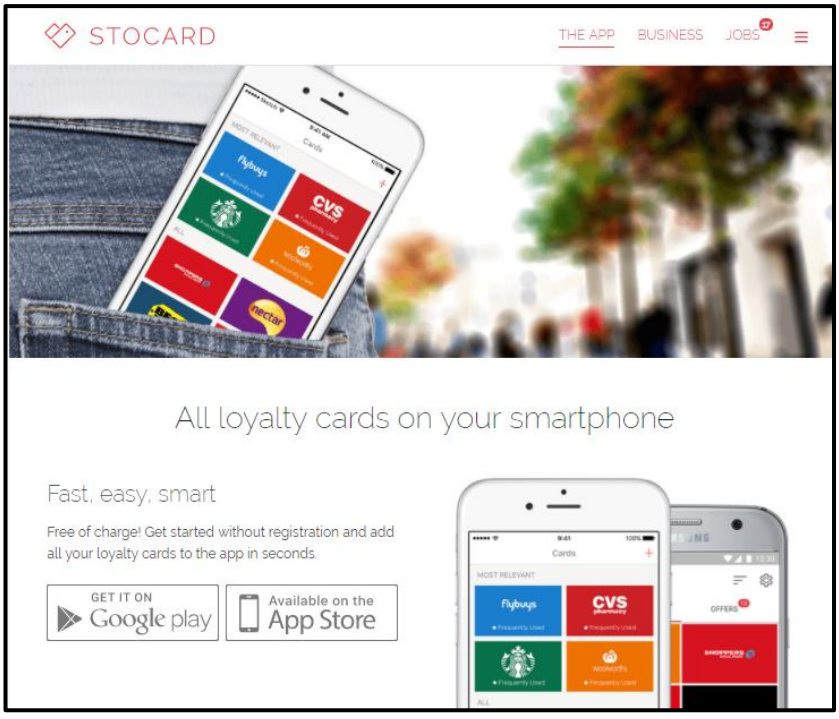
This latest White Paper will review this question and define digital and Mobile IDs and their role in secure governmental services and projects. It also looks at how physical ID cards rather than being simply replaced by these new ID formats, are still a pre-requisite to the overall success of many schemes.

Highlighting some of the latest physical ID technologies and card structures available – and the advantages of these – the opportunity exists for the two styles of ID to work in tandem, with the best of both formats enabling a secure and reliable ID project to be delivered.

A Growing Mobility

Our smart phones have become a key tool in many of our day-to-day activities, helping us communicate, carry out transactions and share information between ourselves and many commercial organisations.

The convenience of the smart phone, together with the growth in software technology and the latest Apps means we are already seeing many traditional physical products being replaced. As an example, Stocard (www.stocardapp.com) allows smart phone users to store all their physical loyalty cards digitally and as their marketing says, 'Simply present your Stocard App and never miss a discount again - ***and all that without plastic cards***.'



The Stocard website presents an app to replace your plastic loyalty cards

Therefore, if physical cards are being replaced in the form of a smart phone app that enables the holder to access the various loyalty schemes, could this also happen for national IDs with the creation of digital and mobile IDs?

Digital ID – A definition

Digital identities have existed for many years in the form of smartcards where the contact or contactless chip contains the relevant holder and scheme information. National IDs, healthcare cards, and driving licences are all examples, however, with the growth in smart phones this concept of Digital ID must also now include Mobile IDs.

Under the European Union (EU) Regulation on Electronic identification and Trust services for electronic transactions in the internal market (also known as eIDAS Regulation) Digital ID is defined as "the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person". [1]

As an extension of this according to the GSMA, the worldwide standards body for governing mobile phones, Mobile IDs are defined as *"an extension of digital identity provided via mobile networks and devices – for example via SIM-based solutions or by using mobile devices, user's attributes and credentials to form part of a personal identity*"[2]

The definition is therefore clear and in a similar fashion to the commercial Stocard application new technologies and providers now exist that allow a person's ID to be extended to a smart phone in the form of a mobile ID. Governments and the public can both benefit from additional functionality, security and privacy options and with the growth in smart phone use then is there still a requirement for a physical ID card?

[1] Regulation (EU) N 910/2014 which enable cross-border and secure electronic transactions and identification in the EU Digital Single Market.
[2] https://www.gsma.com/identity/wp-content/uploads/2015/01/Personal-Data-Regulatory-Overview-2014.pdf

Digital ID – The Challenges

The growth in global smart phone use and the key societal drivers of convenience and ease of use are clear. Alongside the desire to explore commercial and government applications the growth in Mobile IDs appears to be the future, however, it is not without its challenges:

Smart Phone Use – By their very nature, Mobile IDs require a smart phone and whilst their growth has been exponential these are not always within the reach of every citizen due to their initial and ongoing costs. Smart phones are also not mandated and remain a discretionary lifestyle purchase, therefore a National or International ID scheme will always require an alternative to those who cannot afford or don't want a smart phone.

Infrastructure Demands – Similarly, there is a requirement for infrastructure with Mobile IDs as phones and their networks require power to operate. If these fail – be it the smart phone battery life, phone signal, or network itself – then the ability to authenticate and validate a Governmental ID such as a Driving Licence or National ID is lost.

Interoperability and Standardisation – Whilst standards are developing, and definitions exist for Digital and Mobile IDs, the platforms and software protocols to deliver them are many and varied. Selecting the correct solution for a Mobile ID is, therefore, a continued challenge for interoperability across national borders and schemes

Public Trust – Mobile IDs require connectivity through online systems and cloud-based security and these demand the trust of the public. Resistance to online technology by members of the public can create issues for schemes and link with the challenge that not everyone has a smart phone.

Physical Security – A Mobile ID also has no physical security features for the examiner to validate however the need to authenticate a person often requires the ID card to be handed over to the examiner for checking. Mobile IDs present the challenge of this now needing to be the smart phone itself being handed over. Putting the phone power issue to one side, this also requires the constant display of the mobile ID screen, and the need to handover something much more than just an ID card which may present additional privacy and security issues.

A Continued Need for Physical ID Cards

It is clear that physical ID cards therefore still have a role to play in delivering effective identity schemes. Governments and National ID issuers are still using physical ID cards for many applications and services. Their ability to be carried at all times, independent of smart phones or technology, be instantly validated, and easily personalised by issuers make them an ideal solution.

Whilst 2017's ID4Africa government survey found that 53% of respondents expressed a belief that Mobile ID will become more important than physical ID in 10 years, it also reported that most governments still hold the '***strong belief that plastic ID will not be eliminated in the near or mid-term, due to illiteracy and low network and smart device penetration***'.[3]

In certain cases, current legislation also demands that their use continues. In the USA, the REAL ID Act requires all driving licences to be compliant to specific standards in order to enable travel or federal identification by ensuring the ID is authentic. A physical ID card enables this through the smartcard technology which allows the card to be linked back to and checked with its initial issuing agency, alongside the integration of security features to protect the card for tampering and enable authentication by authorities.

In addition to legislation, the carrying of a physical ID also gives holders a sense of belonging and a sense of state or national pride. The unique designs of ID cards help engender this feeling and together with the unique security features included in the design, provide the dual benefit of anti-counterfeit protection and celebration of a scheme or a nation's identity.

Physical ID cards enable the integration of security for instant verification and engender a sense of national identity

[3] http://www.biometricupdate.com/201703/id4africa-releases-results-of-its-2017-government-id-survey

Physical ID Card Options – Security in your Hands

Given the benefits of still having a physical ID card, it is essential that the security within the card is maximised. A variety of substrate and security options are therefore available to card issuers for the production of a credible, secure and long-life ID card that can be easily presented and validated by authorities as an integral part of its design.

Card Structures

People often assume that an ID card is made from a single piece of plastic and cut from a large sheet, but in reality, a typical card includes multiple layers of white & clear PVC bonded together. The top clear layer is used to personalise the card with a photo, name and variable data of the bearer, whilst the internal layers contain the background design and print, including any security features. If the card is a Smart Card it will include electronics – such as a contactless chip or antenna – and these layers are sandwiched in between the other PVC core layers.

A typical PVC Card structure with multiple layers

Composite cards are different from 100% PVC cards in that instead of constructing cards solely with layers of PVC, they utilise a range of different materials to add both the durability and security features demanded. The most common material to add to a Composite Card is PET, where the

PET level can be 20%, 40% or 60% of the total structure. Another example of a composite card would be a PET/PETG Card (PETG core) where the PETG is similar to PVC but with increased resistance to bending. In both cases, the addition of alternative materials adds significant durability to the card structure in comparison to PVC.

The need for more durable ID cards has increased significantly as issuers are looking to maximise the lifespan of a card. Research from MorphoTrust who supply Driver License issuance materials and support to 42 states in the US, identified the move towards more durable cards occurring with the REAL ID federal mandate to better secure state driver licenses.[4]

This has meant that composite cards are now in many cases the go-to option in the high-security identity document market, providing a more durable and secure ID card solution in comparison to PVC. The PET, even at low levels, significantly aids durability whilst a PVC/PETG core will help to keep the overall costs down.

Importantly with these new composite card structures, issuers can use their existing equipment and consumables with a few small manufacturing process changes. For example, composite PET/PVC cards can still be personalised with ITW D2T2 Ribbons and the security and durability of the card can be increased by adding an ITW Laminate Patch or an ITW Overlay.

Another extremely popular card substrate to add durability is Polycarbonate (PC). PC is a thermoplastic polymer with high temperature resistance and impact resistance. PC ID cards are manufactured through the fusing together the different PC layers.

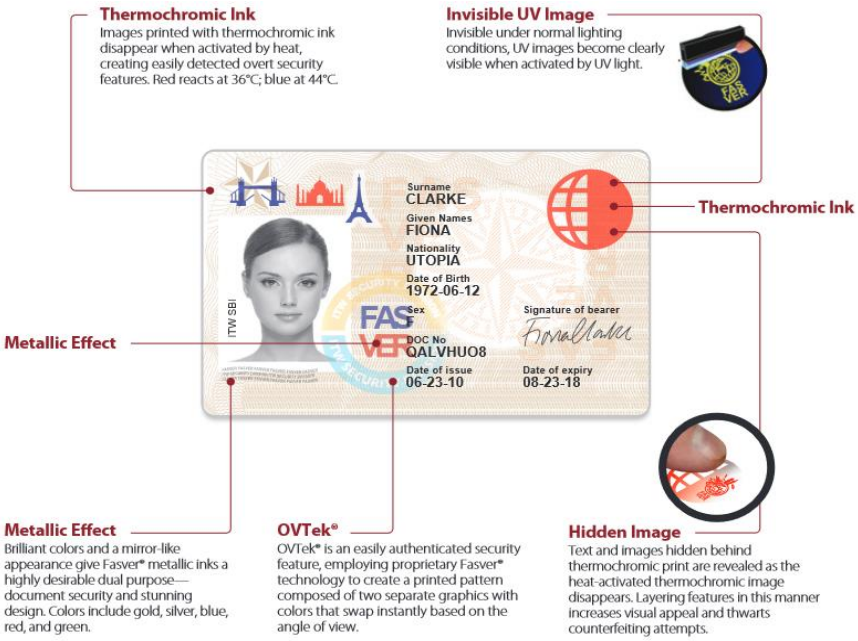
A typical Polycarbonate Card structure

[4] http://www.secureidnews.com/news-item/Card-tech-101-advanced-materials-secure-id-Cards

One of the many layers utilised is a laser engravable layer which enables the personalised data to be added by laser within the card structure rather than being printed on the top surface by a printer. This laser engraving capability combined with the high resistance polymer results in an extremely durable card with many card issuers, such as Gemalto, quoting a lifespan in excess of 10 years for polycarbonate identity documents.[5]

An additional benefit to PC is that its manufacture does not leave behind any dangerous residues and the disposal of any unwanted material does not give off any toxic gasses, meaning the material is regarded as more environmentally friendly when compared to PVC or composite cards. Another major advantage of PC is the ability to embed security features within the many card layers thus making them less susceptible to tampering or counterfeiting including traditional security features such as guilloches/rainbow printing, screen-printing, colour shifting inks, transparent and metallic holograms and ultraviolet inks.

ITW offers a range of products for PC substrates including **HoloPC** (Transparent Holograms), **PC Protek™** (Printed Polycarbonate Layers) and **Unichroma™** (D2T2 Ribbons for PC Substrates). Within PC Protek™, ITW can include some of their unique features such as OVTek® and Imaprotek®.



PC Protek™ security layers enable card issuers to incorporate a wide range of patented and unique security features

[5] http://www.securitydocumentworld.com/creo_files/upload/client_files/polycarbonatejuly20081.pdf

Physical & Mobile ID – The Best of Both

In order to enable access to a wide variety of both commercial and government services, we all have a need to prove our identity in our everyday lives. The growth in technology and solution providers has meant that our smart phones are now often able to meet this need through the provision of mobile IDs, however, there are still a wide variety of situations where only a physical ID card will suffice.

The two formats of ID should, therefore, be seen as complimentary rather than being mutually exclusive. And having both a physical and mobile identity can help to deliver access to a complete variety of commercial and government services, improving mobility and establishing trust between members of the public and service providers.

Case Study – Belgium Itsme Service

Four Belgian banks and three mobile network operators unveiled a mobile ID platform that lets consumers use a single digital identity to access a range of services such as requesting government documents and confirming online transactions using the SIM card on their mobile phone and a unique five-digit code.

The Belgian Mobile ID consortium rolled out the Itsme service linking a number of commercial partners and the federal government. The app works through a smart phone, SIM card and personal Itsme code to create a digital identity. Users are required to enter their personal Itsme code into their phone or if the smartphone features a fingerprint scanner, they can also work using a fingerprint.

Whilst Itsme is designed to enable greater access to services it also is not designed to replace the Belgium eID card. According to Minister of Security and the Interior Jan Jambon. *"You will be able to use your mobile Itsme in all sorts of situations online, but not when it comes to actual physical checks — airports, borders etc.* ***You'll still need your plastic eID card for that.***"[6]

So, in answer to our original question, physical ID cards are very much still needed and ITW's extensive experience in providing security technologies and overlays ensure that it is the ideal partner to support card issuers in their project to ensure a credible, secure and long-life ID card that provides the perfect partner to mobile IDs.

[6] https://www.nfcworld.com/2017/05/31/352916/belgium-gets-mobile-id-platform-that-will-be-supported-on-all-sim-cards-across-the-country

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.