Physical and Mobile IDs — Working Together to Protect Your Identity

Rather than acting as competitive form types, traditional physical ID cards and mobile IDs that have been securely provisioned onto mobile devices (like smart phones or tablets), can most effectively function in harmony, multiplying benefits.

Digital identities in the form of "smartcards" have been successfully used for a variety of government-issued, card-based programs for over ten years, including national IDs, healthcare cards, government employee credentials, and even "smart" driver's licenses. But with the proliferation of mobile phones, the idea of someone's "identity" has now evolved to include mobile IDs.

The GSMA, the worldwide standards body for governing mobile phones, defines mobile IDs 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."[i] New technologies now exist that allow a citizen's government-issued credentials on a physical smartcard, like a driver's license, to be extended to a mobile phone in the form of a mobile ID. This offers both Governments and citizens alike additional functionality, security and privacy options ─ particularly important in emerging markets with widely-dispersed population that also lack the infrastructure needed to deliver card-based IDs, such as certain parts of Africa and Asia. Interestingly, in these instances, an overwhelming explosion of growth in mobile phone usage can also be found. In fact, a recent survey by the GSMA revealed that over one billion more people will use mobile phones by 2020 compared to 2015. Ten countries will account for 70 percent of this growth, with India leading an Asian charge that will account for 55 percent of global subscriber growth.[ii]

But this evolution doesn't mean the end of physical IDs; instead, mobile IDs should be viewed as an extension of authentic, government-issued credentials. In fact, having both a physical and a mobile credential can help to:

- Provide better, faster, more efficient access to government services
- Safeguard privacy by protecting access to personal data
- Improve mobility by using widely interoperable credentials across both physical and logical domains
- Establish trust between the government issuing the digital identity and the cardholder[iii]

In this executive brief, we will outline the benefits of both physical and mobile IDs and how these two form factors will come together to present a highly secure, highly personalized ID that cannot be easily counterfeited, providing significant cost savings to the Governments that deploy them.

Understanding the Continued Demand for Physical Cards

Governments are continuing to use smartcards as national IDs, driver's licenses, voter registration cards, refugee cards, and more. In these instances where greater levels of security are required, physical cards are an ideal solution because they can be easily customized, country-by-country, including adding several in- and on-card security features. For example, in the United States, driver's licenses need to be REAL ID Act[iv] compliant in order to be admitted to a military base or Federal agency, or even to travel domestically. In short, the REAL ID Act requires that a citizen's ID has been issued by a state that can verify that a citizen's driver's license is authentic. One way to do this is to issue driver's licenses on smartcards, which can then be tracked back to a state-funded agency, such as a local motor vehicle registration office.

National ID cards also offer a unique opportunity to include custom security features that engender a sense of national pride: many citizens still attach a lot of importance to having a physical item that shows that they "belong", and the card design is also an opportunity to shine. The use of custom holograms and laser engraving can serve the dual purpose of providing anti-counterfeiting measures while giving unique personalization that is symbolic of that country's cultural heritage.

Why Mobile IDs are the Future

Despite the historical prevalence and preference for carrying physical cards, there is a growing trend of blending a citizen's physical and online identity in the form of a mobile application for commercial purposes. For example, a retail loyalty card app can easily replace a pack of store-branded cards. Likewise, gym membership cards and hotel access keys are slowly but surely being replaced by mobile access applications.

Given this progression, it is hardly surprising that Governments are evaluating ways to migrate a citizen's identity onto a mobile phone in ways that are most convenient for citizens yet, cost-efficient for the agencies issuing the IDs. Australia and New Zealand recently announced a bilateral agreement allowing citizens of either nation to use a mobile token to visit each other's countries. In Europe, a prominent Eastern nation is currently exploring how to integrate mobile IDs into its existing eID infrastructure to expand its Government-to-citizen services within its borders. Finally, in the United States, there is an active request for proposal (RFP) in process to enable the provision of mobile driver's licenses to citizens of a particular state that would aid in compliance with the aforementioned REAL ID Act, and 12 others are in the process of passing laws that would allow the use of mobile driver's licenses within their state.

This trend is happening in some form in many countries around the world today as Governments and relevant authorities look to move ID cards onto users' mobile phones.

For The Highest Level of Security and Convenience, Think Co-Existence

When it comes to highly-secure government applications, physical cards and mobile IDs can work together as part of a total multi-factor authentication solution. For example, tri-factor authentication processes blend physical and mobile security by only granting access to a user after successfully presenting several separate pieces of evidence, notably knowledge specific to that user (something they know, such as a password or phrase); possession (something they have, such as a physical card); and inherent data (something they are, such as a registered fingerprint that can be read by a biometric scanner). As the demand for multi-factor authentication continues to rise in the interest of increased security, so too, will a hybrid approach to credential deployment.

A current example of where the physical and mobile ID "worlds" co-exist is the Irish Passport Card, a highly controlled, highly secure document that allows travel across borders in the European Union. In this use case, Irish citizens can apply and pay for their Passport Card using their mobile phone. Additionally, global banks are allowing customers to order credit cards and other products by simply submitting a selfie for verification purposes. These applications exist because speeding-up the enrollment process dramatically reduces the issuing agency's overhead and administrative costs, while enabling the citizen to have greater convenience without compromising their privacy. In the end, a physical card is still issued, though the security protocols, including authentication of someone's credentials, was done in advance, online, ensuring that the card issued

is a “genuine” ID. We expect that more instances like this combined physical and mobile identification will become more and more commonplace in the foreseeable future.

Transitioning to the Right Secure ID Solution for your Organization

It’s clear that we will continue to see new and different applications of physical IDs converging with mobile applications in the months ahead, including but not limited to mobile driver’s licenses, gun permits, vehicle registrations, or even emergency passports. But physical cards are also here to stay for some time and they can work in parallel with mobile IDs to provide a citizen greater flexibility and security.

HID Global is at the forefront of this trend. Its HID HDP® printers are the clear market leaders in producing highly-secure contact and contactless, multi-function smart cards which can be encoded with data that is specific to only the intended user. Through the use of HID Global’s end-to-end Seos® platform, that same citizen’s credentials can then be provisioned on to a mobile phone using our HID goID™ technology, thus enabling virtually any government-issued ID to be authenticated both online and offline on a smartphone.

If you’re interested in learning more about our ID card printing solutions for Government-to-citizen applications, check out our guide, *Top Ten Considerations for Choosing the Right Secure Issuance Solution*.

Or, if you’d like to learn more about the most advanced Government-to-citizen mobile ID solution, HID goID™, listen to our webinar, The Future of Government-issued Mobile Identities. Find out how we are able to protect a citizen's identity without compromising their privacy.

2017-09-28-pacs-hid-phys-mobile-ids-wp-en PLT-03254

[i] *Mobile Identity: A Regulatory Overview (Second Edition)*, GSMA Personal Data Report, January 2015

[ii] *Global Mobile Trends,* GSMA Intelligence Report, October 2016

[iii] *Mobile Devices and Identity Applications*, Smart Card Alliance, September 2012

[iv] *Real ID Act of 2005*, https://www.dhs.gov/real-id-public-faqs, United States Department of Homeland Security, October 2016