Mobile ID Solutions for Government-to-Citizen Applications

Abstract

This paper looks at how, like everything else in our lives, citizen ID documents such as national IDs and driver licenses, will ultimately follow the trend toward mobility. Since citizens rely upon IDs for everyday scenarios, most are ready to use smartphones to simplify this aspect of life as well. The result is the ability to use a smartphone to carry a citizen ID via a secure, digital credential called a mobile ID.

This paper specifically reviews the infrastructure required to take mobile IDs from concept to reality including new technologies, guiding principles, cross-border interoperability considerations and real use cases.

Introduction

The smartphone has become an all-purpose tool relied upon to share information, make transactions and engage in life's daily activities. While commercial uses of mobile ID credentialing on smartphones have grown rapidly, the government sector remains the last frontier. However this is changing. Citizen demand for smartphones to be their "universal tool" for all their everyday transactions has increased, and the enabling technologies for secure mobile ID are now available and proven. Today, it is no surprise that mobility has converged with citizen identification. Not only do mobile IDs give governments an unprecedented opportunity to provide citizens with new levels of convenience, but they also enhance governmental capabilities to deliver their most important secure ID programs.

In the context of this document a mobile ID is a secure ID credential delivered, by a government to the mobile phone, more specifically to a smartphone, of a citizen. A mobile ID is an all-in-one application for receiving, storing and presenting a citizen's ID with the highest level of privacy protection. It is expected that such a mobile ID will co-exist with a physical document for a long time to come.

A great example of how mobile IDs will positively impact society, globally, can be found in the area of law enforcement. The relationship between police and citizens in any country face its challenges. From a law enforcement perspective, it all starts with the interaction between the police officer and citizen — answering the question: "Who is this citizen whom I am approaching?" A mobile ID that provides secure retrieval of real-time accident, crime or insurance information, whilst protecting the holder's privacy may spell the future of improved police-citizen interactions,especially if such a transaction can be initiated from a safe distance if needed,

As smartphones become ubiquitous — across nations and socio-economic groups — new innovations in secure mobile technologies are facilitating the ability to issue and verify secure identification — quickly, safely and remotely. HID Global is uniquely positioned to lead this shift, providing the secure ecosystem needed to facilitate the provision of citizen IDs to smartphones.

From driver's licenses and national ID cards, to vehicle registrations, residence permits and much more, mobile IDs mark a new era in which citizens will be able to confidently use their smartphone as their secure and trusted IDs and governments can reach a new level of convenience in issuing IDs and extending their relationship with citizens.

HID goID™ : Citizen IDs on Smartphones

HID Global's new goID™ platform leverages smartphones and mobile IDs to do the work of a secure government-to-citizen ID. HID goID™ allows smartphones to be used for identification purposes, but also for transactions in ways not

possible with a plastic ID card.

A mobile smartphone phone using HID goID™ enhances a citizen's day-to-day experience. Imagine how HID goID™ may impact travel. Today, citizen's use a national ID or driver's license at the airport for domestic travel, but also carry a boarding pass separately on a phone or a piece of paper. With HID goID™, the two converge - providing greater security, convenience and flexibility for both the citizen and the authenticating party. Rather than in wallets, IDs can now be securely stored on smartphones.

With everything on the smartphone, citizens may choose to leave their purse or wallet at home. Citizens will also be able to control when and how much information is shared, allowing them to protect their privacy. For example, when a citizen is purchasing age-restricted goods, they only need to provide their photo and age — none of the other personal information usually loaded and freely readable on a physical driver's license needs to be shared.

HID goID™ can allow citizens to renew their driver license remotely, eliminating the need for people to stand in lines for new cards and renewals. This is also good news for government agencies, which can do their jobs more efficiently.

Making Identity Easy for Government Agencies

HID goID™ is perfectly placed to provision mobile IDs directly into citizens' mobile phones for offline verification. Unlike other solutions that rely on wireless cloud connectivity for verification, HID goID is always verifiable, no matter the connectivity to the cloud. This is extremely important in the case of national and public security, where identity needs to be securely verified – HID goID™ can securely verify both online and offline.

HID goID™ is flexible and built on open standards for security, enabling interoperable solutions to be found where identities can be signed in one jurisdiction, but validated in others -- for example, a driver's license produced in one state but validated in many.

A New Level of Real-time Connectivity and Computing Power — HID goID™

- Facilitates the delivery of citizen-centric services, building trust and convenience;
- Allows them to issue, revoke or change mobile IDs more efficiently, securely and quickly;
- Improves law enforcement interaction with citizens;
- Prevents counterfeiting through electronic authentication;
- Works across multiple platforms and operating systems;
- Opens the door to new revenue opportunities; and
- Can be easily and securely verified, both online and offline.

What will it take?

To be able to deliver a mobile ID a full range of security implications need to be addressed.

Provisioning:

- Know with certainty who is applying
- Protect all information
- Securely send mobile ID to correct device
- Once on device, mobile documents can't be modified or accessed
- Real authentication by relevant authorities
- Ability to revoke, edit, append data (e.g., adding an infraction to a mobile Driver's License)

Privacy:

- Assurance that no one else has access to personal data
- Can't track identity (just as with card in pocket)
- Need to segregate applications
- Verifying entity should not need to touch the device

Once the mobile ID is on a mobile device, authorities must be able to verify authenticity in a variety of scenarios. Specifically, officials must be able to verify:

- It belongs to the citizen.
- It's genuine.
- It's still valid.
- It's not a fake ID.
- It's been issued by the relevant authorities.

Mobile ID Fundamental Policy Principles

There are six principles government organizations/agencies and citizens, alike should adhere to for a successful transition to mobile IDs:

1) **Voluntary**. Participation is voluntary; user controls sharing of information and device.

2) **Interoperable.** Works with major smartphone handset manufacturers and operating systems and is viable across jurisdictions, states, provinces and continents.

3) **Secure.** Strong standards-based cryptography platform and citizens' data can only be viewed by the intended authenticating smartphone.

4) **Private.** No one else can access personal data or track identity; must be able to verify data without handing over the physical smartphone.

5) **Remote-Capable.** Citizens' mobile IDs must be securely available, even in remote areas without internet or telecommunications networks — including the provisioning, updating or revoking of credentials.

6) **Always Available.** When a citizen's smartphone is inoperable (i.e. dead battery) it is still possible to securely access the ID.

HID goID™ addresses all of these principles and more, assuring governments that mobile IDs will empower citizens to enjoy convenience and simplicity while delivering the security and privacy expected in a trusted government-issued credential.

Mobile ID Infrastructure

The following diagram depicts the components of a mobile ID infrastructure:

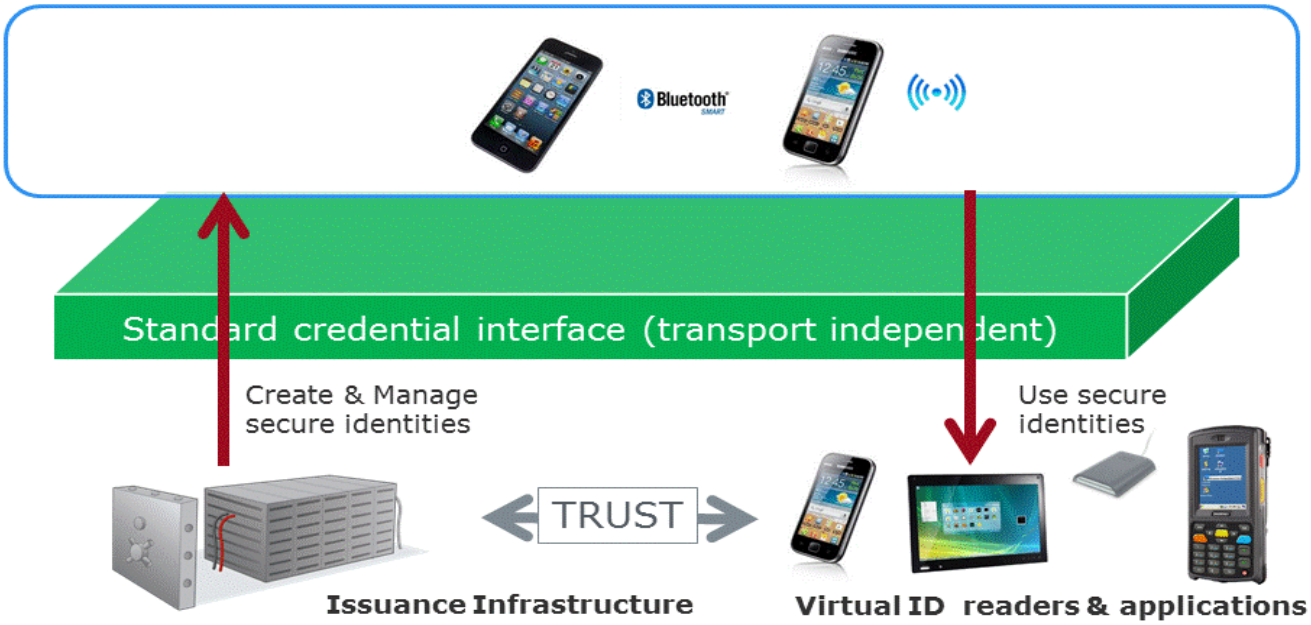

Fig. 1: Mobile ID Infrastructure

- **Issuance infrastructure**. The set of components at the issuance authority (e.g., the DMV for a driver's license, or central government for a National ID card), that manage the lifecycle of secure mobile identities including the creation and management of the IDs. The issuance infrastructure also incorporates the necessary management functions to confer trust into the mobile ID itself while also validating devices like mobile ID readers. This is important because other standard mobile devices with BLE or NFC capabilities could potentially be transformed into a trusted mobile ID reader by conferring trust (keys) to it via the issuance infrastructure.
- **Standard transport-independent credential interface.** This allows both the issuance infrastructure and the validating devices to interact with the mobile ID on a citizen's smartphone. It is imperative that this is as transport-independent as possible to ensure compatibility with next-generation proximity communication technologies.
- **Mobile ID readers and applications:** These must be capable of interacting with citizen smartphones using a secure, standard interface while also being able to verify the mobile ID. Reading endpoints should be considered "trusted endpoints," capable of securing the key material that confers trust between mobile devices.

Limitations of a Secure Element Approach to Citizens' Mobile Devices

There are several significant limitations to using a secure element approach to mobile IDs on citizens' smartphones.

Interoperability Limitations

To issue a mobile ID to a secure element on a citizen's smartphone (e.g. SIM or embedded secure element) the issuance agency must integrate with either a mobile network operator (MNO) which issues the SIM or an original equipment manufacturer (OEM) which issues the handset and embedded secure element. The MNO and OEM control the keys that allow the loading of the mobile ID applet onto the respective secure element. This includes the keys required to

personalize the mobile ID — such as those that send unique citizen-specific data elements, images and authentication. To do this, governments and/or issuing agencies have two options:

1) Integrate with all of the MNOs in the country; or
2) Partner with a Trusted Service Manager (TSM) which has already integrated with all or most in-country MNOs.

Costs include the creation of contracts with MNOs and TSMs as well as the per-unit cost to load the mobile ID application onto the secure element and subsequently personalize it.

In the context of this paper, it should be noted that the use of a secure micro SD card (µSD) that also contains a secure element is not an adequate global solution because the ability to read such cards are not universally available on all handsets.

Privacy Limitations

Currently, the most used technology for secure elements is based on a Java card secure element with GlobalPlatform[i] device technologies. This approach allows for multiple service provider security delimitations using security domain concepts.

This said it is possible for non-trusted mobile ID readers to:

1) Discover the presence of a mobile ID applet (using the SELECT command with the right applet ID-AID), and
2) Freely read a unique number (Chip Serial Number).

This means unauthorized readers could potentially track and correlate a specific citizen using these unique identifiers.

This should be considered a limitation with respect to Mobile ID Fundamental Principle number four which states, “It should not be possible to track the identity of citizens or - from untrusted endpoints - gain knowledge that a smartphone carries a mobile ID.”

ASSA ABLOY / HID Seos® and Mobile IDs

HID Global’s goID™ builds upon a proven mobile ID ecosystem with HID Global’s proven Seos® technology at the heart of the solution. Seos is a cryptographic infrastructure technology that has been developed specifically for the mobile experience, i.e. for provisioning secure credentials over the airwaves to smartphones and mobile devices.

The HID goID platform enables instant over-the-air provisioning and streamlined access to cloud-based government information services with the assurance that all transactions are secure and trustworthy. All transactions related to issuing,

managing and presenting credentials using mobile phones are conducted in a highly secure environment protected by end-to-end encryption.

HID Global Seos / HID goID™ is:

- **Mobile.** Seos enables secure identities to be truly mobile. A user’s identity is no longer hardwired into a piece of plastic, but can be digitally encoded onto a phone or a wearable. Seos enables any smart device to become a credential without requiring a Secure Element.
- **Interoperable.** Seos enables an open ecosystem in which credentials and readers from different manufacturers can communicate over NFC or Bluetooth Smart, making it truly independent from the transport technology and the transport security model.

- **Secure.** Seos uses standards-based cryptography to enable the provisioning of secure identities. Seos protects the storage and use of those secure identities across a broad range of credential and mobile OS platforms. It is based on strong mutual authentication between the application on the citizen phone and the reading device. Protects against 'man in the middle,' reflection, reply and other attacks.
- **Private.** Seos ensures that no information that might be used to identify or track the credential holder can be read by an unauthorized party. Specifically it is not possible to freely read a unique identifier nor possible to even discover the existence of the Seos-based virtual ID on a smart phone.

HID Global's breakthrough Seos credential technology powering mobile IDs is already widely deployed by organizations seeking a convenient yet secure way for people to access office buildings, hotels, college campus and healthcare facilities and more. HID Global's Seos technology is embedded in Starwood Hotel Group's Preferred Guest App (SPG), enabling guests to access hotel rooms via a mobile key on their smartphones in hundreds of Starwood locations around the world. Guests simply receive a secure Seos mobile ID with their room number via the SPG app before arriving at the hotel, allowing them to bypass check-in and proceed straight to their room (spgpromos.com/keyless).

The criteria for a citizen to receive and use a secure mobile ID is very demanding, similar to what a hotel guest needs to receive and use a secure mobile room key. HID Global is using this same proven technology to bring mobile IDs to citizens' smartphones.

Seos: A Multi-layer Security Approach

Security for mobile IDs is based on a multi-layered approach comprised of security technologies that run across the citizen smartphone, the verifying device (app) and the issuing infrastructure.

- **The citizen smartphone.** Seos can be run and has been tested on secure elements and in pure hardened software credential storage. The latter being preferred to secure mobile applications because currently there is no common hardware security supported across all mobile platforms. This means the digital keys in the mobile phone are independent of any partner system from MNOs and OEMs (see Section 3.1).

  Using a hardened software-based credential allows HID Global to benefit from the many built-in security features of a mobile phone operating system. This allows applications to store information and operate securely. In addition to this, mobile IDs are stored as SIOs, (Secure Identity Objects) which are encrypted and signed using NIST Suite B approved cryptography, making it impossible for a hacker to create or modify the content of a mobile ID. Mobile IDs based on HID goID™ are tied to the device through a diversifier and device-specific cryptographic keys (there are no master keys). This means a citizen's mobile ID will not work on another device. The app itself includes binary protection including root detection and anti-hacking techniques for reverse engineering, tampering, unauthorized access, code injection and security by obscurity.

- **Transactions between citizens' smartphones and the verifying (reader) device.** HID Global's Seos technology does not depend on the security of the transport technology; it is standards-based and includes secure messaging, strong authentication and data confidentiality. With HID goID™, transactions between citizens' smartphones and verifying readers rely on the Seos secure messaging protocol to secure over-the-air communication independent of the transport technology (e.g. NFC or Bluetooth Smart).

  Every Seos transaction is unique and cannot be cloned (recorded or replayed). Seos is also resistant to man-in-the-middle attacks, reflection attacks, replay attacks, message deletion, message reordering, message modification, message concatenation and message insertion. Further, HID Global's Seos protocol supports strong privacy, meaning that it is not possible to track the identity of a device.

- **Issuing infrastructure:** The issuing infrastructure processes incoming mobile ID payload securely issuing and protecting the citizen-specific data using device independent diversified keys that are managed and generated within Hardware Security Modules (HSM). Citizen-specific payload is securely wrapped and sent to the citizen's smartphone using different transport channels. The issuing infrastructure also manages all keys including the

issuance to verifying devices — ultimately allowing them to become trusted endpoints.

The security of the issuing infrastructure is multi-layered:

1) Other systems can connect to the issuing infrastructure using TLS1.2 enforcement, cypher suite control and/or certificate pinning.

2) End-points are protected with routing detection capabilities, code obfuscation and third party penetration tests of the overall system.

Mobile ID Interoperability Model

Beyond the security of a single mobile ID and its interaction with the verifying device as illustrated above, there is another important component to the verifying infrastructure. Widespread adoption of mobile IDs requires interoperability between issuing authorities across agencies, borders and geographies, worldwide. For example, the use of mobile driver's licenses across state lines in the Unites States provides a good example of why interoperability is so critical. At the most basic level:

- States must issue a mobile driver's license that can be read/verified by authenticating authorities within any of the 50 United States.

- Similarly, States must have the capability to read/verify mobile driver's licenses issued by other States.

Lessons Learned from the US PIV Standard

While standardizing to ensure interoperability in the reading and authenticating of mobile IDs is a necessity, we can learn from previous attempts to achieve a depth of standardization which risked cannibalizing the bigger market opportunity. Specifically we are referring to the United States' PIV standard[ii] which was used to grant access to Federal facilities and information systems and assure appropriate levels of security for Federal applications. PIV standardized not only the data model and interface but also most of the transport and data retrieval methods including set guidelines. While excellent in concept, the world did not wait for the PIV standard to be perfected. The world kept evolving and innovating and by the time the standard was published the mobile revolution had begun. Unfortunately mobility was not a part of the PIV roadmap. While newer versions of the standard have adopted some mobile capabilities, the world is already moving on with the wearables revolution, and even the more mobile friendly PIV evolution is ultimately limiting in some use cases.

So what does this suggest as we launch our mobile ID platform,* HID goID™*?

A better approach would be to define security requirements for the data model and interface but not tightly standardize the transfer protocol. The data model would be standardized potentially by NIST[iii], ISO and/or ICAO and the security of the data would rely on asymmetric signatures, similar to the model of the federal CA bridge. This would allow new technologies, to be developed for current smartphone technology but at the same time evolve to keep pace with innovation. In this example interoperability is provided at the data model and interface level.

Related, to avoid a monopoly, governing bodies of specific mobile ID categories (e.g., mobile driver's licenses) must adhere to a set of principles. Specifically, the secure read protocol (interface):

1) Must be openly available for all, including a reference implementation with source code over a specific transport (e.g., Bluetooth Smart); and

2) Must be licensed by the protocol provider under RAND (Reasonable and non-Discriminatory) terms.

In the case of mobile driver's licenses, following these principles will allow the verification applications from different States to embed the transport protocols from the other States (or technology providers) to insure seamless interoperability.

Conclusion

An important step toward making the vision of mobile citizen IDs a reality, the HID goID™ platform enables federal, state and local government agencies to issue credentials over the air to citizens' smartphones for driver licenses, passports, social security cards and other national ID documents. It also makes it possible for a smartphone to serve as an all-in-one secure credential and ID reader, providing the choice to rationalize ID readers on to a standardized smartphone platform at border crossings and other locations.

In an age of global insecurity, citizens can be assured that mobile IDs powered by HID goID™ are backed by proven technology — empowering them to enjoy the convenience and simplicity of a mobile ID with the security and privacy expected in a government-issued credential.

With HID goID™, HID Global is able to provide government agencies/organizations with credentials on mobile devices that:

- Can be securely provisioned, modified and revoked
- Protect the privacy of the individual
- Work across multiple platforms and operating systems
- Can be easily and securely verified, both online and offline

Successful adoption of mobile IDs requires the interests of both governments and citizens be taken into account and therefore the need to adhere to fundamental principles: voluntary, interoperable, secure, private, remote capable and always-available.

Connectivity sets today's standards for communication, information and transactions. HID goID makes it possible for governments to reach a new standard in their relationship with citizens – whether the interaction is with law enforcement, motor vehicle agencies, educational institutions, or quasi-governmental organizations.

To learn more about how HID goID™ can help you address your government-to-citizen mobile ID requirements, or to arrange for a pilot program, contact your local HID Global Government ID Solutions representative.

2016-05-10-hid-govid-mobileIDsolutions-wp-en PLT-02884

[i] GlobalPlatform: "The standard for managing applications on secure chip technology." http://www.globalplatform.org

[ii] NIST FIPS 201: "Personal Identification and Verification." http://www.nist.org/nist_plugins/content/content.php?content.49

[iii] NIST FIPS 201-2: "Personal Identity Verification (PIV) of Federal Employees and Contractors." http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf