Overcoming Objections to Smartphones as Your Credential

Security Industry Association

By Suzi Abell, 3xLOGIC on September 14, 2018

Could the phone replace your access control card or fob?

Moore's Law notwithstanding, technology advances have always outpaced our ability to adopt and consume them. This has been and remains the case with even the least complicated aspects of technology like electronic access control (EAC). At their most basic level, EAC systems lock and unlock the door, a simple task until you mix in people who need schedules and rules and exceptions to the rules and on it goes. It is often difficult to drive the desired behavior and this is particularly true with the credentialing that is an integral part of an EAC system. Initially, a credential might have consisted of a simple numeric code that was entered into the lock, often referred to as a cipher lock, thus allowing access. This was a terribly insecure and difficult-to-manage solution, and has since evolved into physical credentials, which expanded to include fobs, proximity cards, biometrics and now a smartphone app playing the role of credential.

With the introduction of biometric and smartphone credentials, the lifespan of legacy physical access control credentials is quickly reaching an end. A convergence in physical and logical access control is driving completely new and different behaviors, as evidenced by the entry of players such as August, which was recently purchased by the largest lock and credential company in the world, Assa Abloy. This aquisition demonstrates validation for these changes in the way we provide access to our facilities.

Smartphone as Credential: The Only Way to Go?

In an ever-accelerating trend, estimates show that 90 percent of the wireless locks sold are integrated with other smart devices. It's no longer necessary to struggle to manage a variety of insecure and vulnerable physical credentials when you can manage all of that through a mobile app. As this market expands into non-traditional access control applications, the necessity for an access control credential on an ubiquitous mobile device becomes mandatory. In the very near future, everyone will carry a credential of some sort, and a mobile credential, housed on a smartphone, is a highly viable way to address these needs.

There are four main drivers for a smartphone as your credential:

- Smartphone-based credentials are inherently more secure
- Smartphone credentials can do so much more
- Smartphone-based implementations can significantly reduce installation costs
- Smartphone-based credentials are nearly impossible to clone

Objections Real and Overblown

For any new technology, there will be naysayers. Some of those dragging their feet object because the new technology threatens their business models. Others just don’t like change or tend to evolve ever so slowly. However, other objections do have validity and need to considered. How can you tell the difference?

Since the potential for smartphones as your credential burst on the scene a few years ago, much has changed. What were once valid objections or limitations have now been surmounted. Some examples:

- Cards Are Cheap: Mobile phones, even inexpensive ones, are roughly 20-40 times the cost of a card. And the cost of maintaining a phone is much higher, requiring frequent recharges and software updates while a card remains very inexpensive and essentially free to maintain once issued. Reality: Mobile credentials have the potential to make credentials more affordable by leveraging an asset that the vast majority of people already have (see http://www.pewinternet.org/fact-sheet/mobile/). In addition there is the potential for reducing shipping and labor costs from managing cards that are frequently lost and/or misplaced.
- Bring Your Own Device (BYOD) Is Awkward: BYOD, or the fact that users leverage their personal phones for commercial uses, presents numerous problems, from network security to whether or not phone owners are willing to permit employer provisioning and/or management oversight. Reality: BYOD is a fact of life, and while personal devices will bring some complications, how often do you hear of a company issuing an employee a phone? And if a company does provide a phone, it’s now a smartphone that can deliver a mobile credential in a corporate-controlled environment. The security industry is not the only one seeing this change. Retail is moving toward near field communication terminals to allow customers to use their smartphones in place of their debit/credit

cards through Apple Pay, Samsung Pay and Android Pay Apps.

- Ongoing Service Billing: What happens if the phone bill is unpaid and the employee incurs service interruption? Reality: Smartphones have become so ubiquitous and, for nearly every employee, so essential to day-to-day, hour-to-hour operation that one's phone bill is probably the very last bill a person will leave unpaid.
- Technology Limitations: The wide range of technical issues that can go wrong with a mobile phone cannot be easily dismissed. Even problems as basic as battery power, operating condition, reliable function and even multi-tasking demands need to be considered. Reality: Everybody has a smartphone, and we all use these devices for so many essential functions today that there is ample incentive to make certain one's phone is operating in top condition.

Having dispensed with the above objections because they have been taken care of by time or technology advances or both, there are objections to smartphone as credential that do require further examination and discussion.

Valid Objections Have Their Day

The objections covered above are no longer valid in slowing down smartphone as credential adoption. Are there other objections that we must deal with? Yes, and they are as follows:

- Physical Revocation Uncertainty: Unlike plastic credentials that can be turned in and physically repossessed when employees are dismissed or turn over, mobile credentials must be remotely invalidated on a device that may remain unseen. Reality: A good mobile credential solution should not depend on sending an update to the phone to disable a credential, that should happen in real time whether the phone is connected or not. An efficiently-designed mobile credential integration will not depend on access to the physical mobile device to activate or deactivate the credential. In reality, access is granted by the interaction between the mobile credential and the extended access control (EAC) system. If the credential is deactivated in the EAC system, then access grants are denied without regard to the type of credential presented.
- Awkward or No Picture IDs: Unlike physical cards that are often printed with the user's picture, name and other basic identity details, these are very often hidden or obscured by phones. Reality: Yes, calling up a photo ID on one's phone does take more time than flashing a badge. But consider that many companies no longer even print identifying information on a badge for fear that the wrong person will get control of that badge and gain unauthorized entry. There are two main uses for badge pictures and two main philosophies around putting pictures and identifying information on credentials.

- Worn and visible at all times so a person can be readily identified as belonging.This is an area a mobile credential does not address.

- To verify that the person passing a secured portal is indeed the person to whom the credential was issued. In this case, it's better to compare the photo stored in the system to the person, instead of a relatively-easy-to-forge picture on a badge. Also, a good mobile credential solution can implement multi-factor authentication (MFA), delivering much greater assurance that the person is who they should be.

  Perhaps the most secure solution is to use a mobile credential for access and have PVC cards printed with the person's badge picture etc. that are just for visual verification and are not credentials.

Possible Other Objections

- Takes too long to get through a door. The objection is that the user must pull out the phone and then launch an app. Reality: For mobile credentials that do not require close proximity to a reader, they will drive a change in behavior as users realize they can initiate the request as they approach the door, with the door unlocked by the time they reach for it. This negates the extra time required. Watch-based extensions to mobile credential apps also promise to speed up the process.

- Phone could unlock remote doors. Some people don't like being able to unlock doors 20 miles away, or even the potential to remotely unlock doors. Reality: A good mobile app should support geofencing to require users to be close to the door they are attempting to access.

- Traditional credentials formats are always on, but phones can be turned off. The objection is simple: Users' phones can often be turned off and are therefore not appropriate as a credential. Reality: The average person has a high level of incentive to always keep their phone on and to know where it is. Why? Think of all the apps nearly every user is accessing on a minute-by-minute basis: A user's phone has their credit card, Facebook, Twitter, instant messaging, email and texting, navigation, to-do lists, camera, music and calendar, and the list goes on and on and on.

Benefits of a Mobile Credential Solution

- Mobile credentials are inherently more secure.
- Credential holders are unlikely to share their mobile devices with others.

- Mobile users are very aware of where the devices are at all times.

- It is very difficult to clone a mobile device/mobile credential.

- Mobile credential apps expand the capabilities of the EAC system.

- Group notification/mass notification can be implemented directly to the credential holders' mobile devices.
- Tracking of the mobile device can provide real-time location information for added security.
- Mobile credential app can quickly become a bi-directional communication channel for personal security (PERS).

What's Your Single Largest Security Risk?

Forget about high-security credentials such as MIFARE and sophisticated certificate handshakes. The single largest security risk for access control is a valid credential in the wrong hands. When that happens, it doesn't matter if it's a 125KHz "dumb" prox card or the most sophisticated smart card; a potentially malicious user now has access, and no one will know if that lost card isn't reported.

The smartphone as the credential is significantly more secure because of one simple fact: People may not know the location of their access control credential at any given time, but they are intimately aware of the location of their smartphone at all times and this location can be tracked. Users are naturally much more careful as to whom they allow to hold or use their phone.

The World of Mobile Credentials

So, how is the world of credentials changing forever? A smartphone-based credential can be and do so much more. In the near future, we'll start to see features such as:

MFA

Smartphones already implement MFA. Soon, new mobile credential implementations will allow administrators to require a screen unlock pin/biometric/gesture to set up a mobile credential, thus implementing MFA with no new hardware at the door.

Mass Notification

A credential – supporting two-way communication with active notification capabilities – can be leveraged to send automated or ad-hoc notifications to users. Add location services and geofencing capability, and you can send notifications only to those people who are within a specific geographic area. And you can further target those notifications to specific people.

Location Awareness

Stop treating a smartphone like a legacy credential; no one should ever "badge" a phone at a reader. By using location services, administrators will define how near to the door a person must be to request access.

Virtual Buttons

With an app for users that uniquely identifies them, why not give them more? We'll see the ability to add virtual buttons to an app to perform functionality specified by the administrator – and such buttons/functions will only be distributed to those allowed to use them.

Personal Safety/PERS

A mobile app that functions as the user's credential and provides two-way communications with a central monitoring station will also provide a path for two-way emergency communications. For example, an employee leaving the building at the end of the shift on the way to her car can quickly and easily ask for assistance or notify security of a potential issue remotely via the mobile device in her hand.

Revoking a Credential

An administrator can disable a user's mobile credential at any time from the server with no need to access the actual smartphone. The smartphone app knows how to submit a credential request but has no idea how to unlock a door. Additionally, administrators can also remotely wipe smartphones of the mobile credential and related apps connected to a corporate network.

Lower Costs and Added Features

Finally, let's consider cost. A smartphone credential adds significant functionality over a traditional credential and is always upgradeable to add new capabilities – all for the same cost, or less, as that of traditional credentials. Also, users do not require a reader to enter a door, so enterprises can eliminate readers on most doors to keep the entrance looking clean and to reduce installation costs.

Over the next 24 months, we will witness unprecedented changes in the tools and services you use every day, and one of those tools will be your access control credential. The security of a door is only as strong as the management of the credential. It only makes sense for that critical credential to be secured inside the most highly encrypted device – your own smartphone.