WHITE PAPER

Best Practices for Integrating Mobile into the Access Control Architecture

Merging Security and Convenience with Mobile

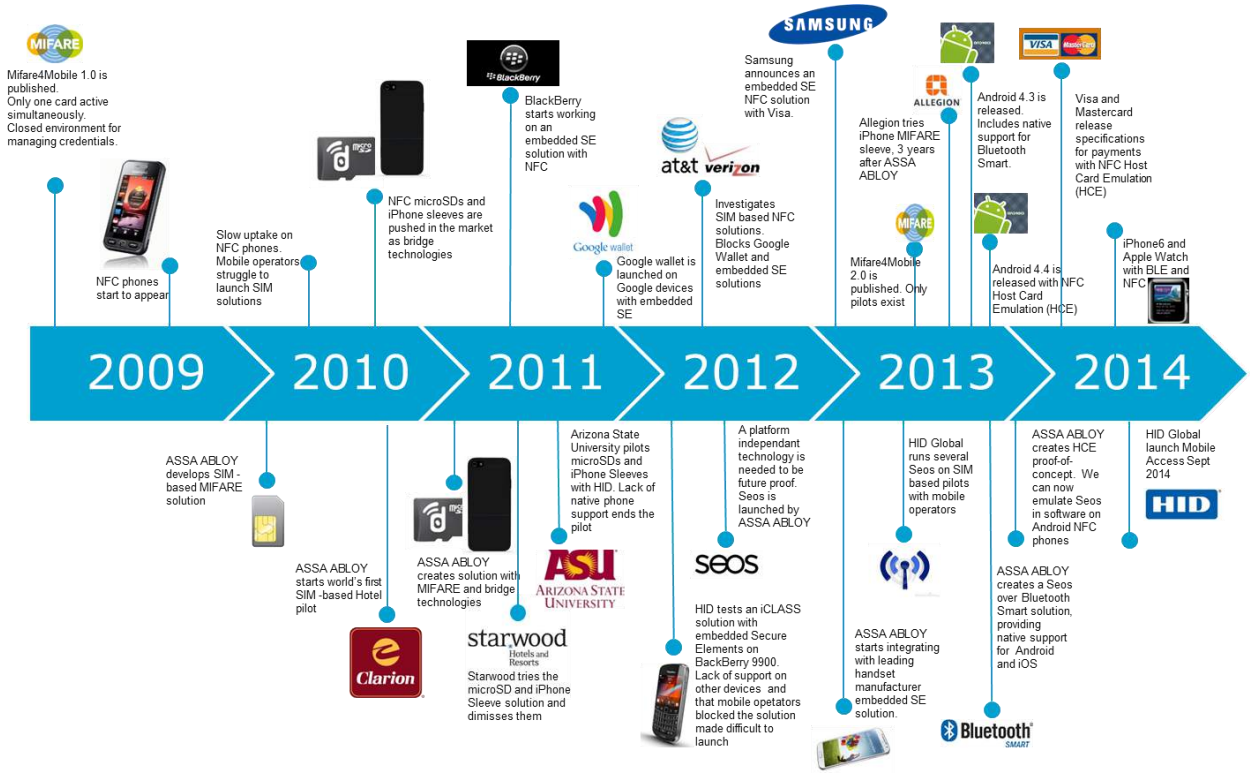
Mobile Access

Using a mobile device to gain access to different buildings is not only about solving a particular problem. It is also about doing things better, by embracing technological advances and delivering a concept that will change how we interact with readers and locks and open doors using our mobile devices. In the era of mobility and cloud computing, enterprises and individuals are increasingly concerned about the security and protection of their physical environment. Correctly implemented, mobile access has the potential to change how we open doors as it's the first time in history we have a solution which can increase both security and convenience.

Mobile Trends

The mobile industry is known as one of the most innovative and fast-paced and what we have seen in recent years has been nothing short of remarkable. Industry research firms project that the number of shipped smart connected devices will grow to 1.7 billion units in 2014. This rapid growth is affecting the underlying technologies and standards in mobile devices as more people use their devices in their daily life and new applications are developed. At the same time, much of the technology used in mobile devices today had been around for quite some time before being accepted by the mobile community. Bluetooth® was introduced in 1994 and it took 15 years before it became a de-facto standard in mobile devices. Browsing the internet on mobile devices has been possible since the beginning of 2000, but it was not until the introduction of the iPhone® in 2007 that the use of a mobile device as a connected computer became widespread. NFC was introduced in the Nokia® 6131 in 2006 and since then most device platforms have added support for NFC; nevertheless, the number of launched services based on NFC has been less than impressive.

Opening doors with mobile devices is not a new idea. Early technology tests were performed in the beginning of 2000 to make payments, ride the subway and open doors and in different parts of the world solutions have been made available to the public. Interest in contactless services has always been high, but creating the user experience and added value that end-users expect has proven challenging. Using an existing payment or access card is in many cases perceived as workable enough, while the relevant underlying technology has made it difficult to launch services that can scale.



There have been many different approaches to enabling mobile access control using different technologies such as microSDs, add-on sleeves, MIFARE® Classic, NFC Peer-to Peer, and Bluetooth Classic, each with their unique sets of challenges. History shows that it is essential to have an architecture that is both agnostic to underlying technologies, such as NFC or Bluetooth Smart, and adaptable to any new trends in the ever evolving mobile industry.

Technologies that support mobile access today

Confidence and education in the use of contactless applications and technologies such as NFC, Bluetooth, mobile wallets, iBeam™ and iBeacon™ are continuously growing and so is the understanding of what technologies are best suited for mobile access control. No matter what the technology, mobile devices offer an unparalleled way to change the way we open doors. However, security administrators and IT directors will need to review which mobile-related technologies will allow them to best engage with their employees to create the optimal access experience on their premises.

Near Field Communication (NFC)

NFC was developed to address the dilemma of multiple contactless standards but its introduction into mobile devices has been less than smooth. Emulating a contactless card on a mobile device was up to very recently only possible via a Secure Element (SE), such as a SIM card. An ecosystem in the form of Trusted Service Managers (TSM) had to be setup to support the SE centric model which resulted in complex technical integrations and business models which made it difficult to launch contactless applications based on NFC.

In 2013 Google® introduced a new NFC feature in Android™ 4.4 called Host-based Card Emulation (HCE). HCE allows a contactless card to be emulated in an App without dependencies on a SE. With HCE it is possible to launch NFC services in a scalable and cost-effective way as long as a standards-based card technology is used.

Visa® and MasterCard® have released specifications on how to do Visa payWave® and MasterCard PayPass™ transactions using HCE, and HID Global® has launched a mobile access control solution with HCE based on Seos. HCE will make NFC more accessible and versatile, so that developers will then expedite services to market which, in turn, will stimulate consumer familiarity and encourage adoption. At the same time, however, the iPhone is a very popular device in the enterprise segment and many are used in organizations around the world today without NFC support. The number of installed Android 4.4 devices is growing fast, but with the lack of NFC in the iPhone 4 and iPhone 5, coupled with the fact that NFC support in the iPhone 6 is currently only available for Apple Pay™, there is still questionable market penetration for HCE-based solutions.

NFC Host Card Emulation

- Standards based contactless cards can be emulated by an App
- Works with NFC enabled readers if a standards-based card technology is used
- A good solution where a Tap experience is preferred
- Not supported by iPhone

Mobile operating systems with support for NFC Host Card Emulation

- Android 4.4
- BlackBerry® 9 and 10

Bluetooth Smart

Bluetooth Smart was introduced into the Bluetooth Standard in 2010 and, having gained a lot of traction in markets such as healthcare and fitness, is now finding its way into the payment and coupon redemption industry. One of the success drivers for Bluetooth Smart is the support the technology has received from Apple, who has supported Bluetooth Smart since the iPhone 4S. Google added Bluetooth Smart to Android 4.3 and as of October 31, 2013, Bluetooth Smart is the only contactless technology capable of supporting a service on the two major mobile operating systems, Android and iOS. Its low power consumption, eliminating the need for pairing and the long reading distance makes Bluetooth Smart an interesting option for mobile access control.

Bluetooth Smart

- No requirement for pairing and low power consumption make Bluetooth Smart, combined with a standards-based contactless card technology, a good technology for enabling mobile access
- Readers may be placed on the safe side of the door or hidden
- Open doors from a distance as you park your car, or if you want to open the door for someone ringing the door bell
- Configure readers including firmware with a Bluetooth Smart- enabled device (such as a phone or tablet)

Mobile operating systems with support for Bluetooth Smart

- iOS 7 and 8
- Android 4.4
- BlackBerry 10
- Windows Phone® 8.1

With mobile access technology continually evolving, it is best to ask the mobile access product vendor for a list of supported handsets in order to assess and compare products.

Transactional experience

Rarely misplaced and consistently in hand, the mobile device has become the most valued technology we own. Using mobile devices to open doors is moving physical access control forward and merges security and convenience. The longer read range with Bluetooth Smart opens up new whole ways to open doors and offers new options for where to place readers. A door can be unlocked upon approach, for a quicker and smoother experience when entering a building. Having Bluetooth Smart-enabled readers in parking garages has proved to be much appreciated; instead of rolling down the car window and reaching out of the window to access a reader, it is now possible to gain effortless access while driving up to the gate. For some types of doors, like conference rooms where multiple readers might be located in close proximity, a tap-like experience with a physical card might be a better option, to ensure that the correct door is opened.

Architectural ingenuity is pushing building design in bold new directions and the traditional reader placement next to the door might not fit in an office constructed mainly of glass walls. Readers and locks, typically placed on the outside of doors, may also be targets of vandalism. Combining the long read range of Bluetooth Smart with a directional antenna can increase security by mounting readers on the safe side of the door, and for aesthetics, readers can be placed out of sight.

Given the nature of contactless technologies, the reading distance can vary depending on the environment where a reader is placed. In an elevator, the reading distance can be greatly amplified by the surrounding metal. The type of smartphone used can also affect the reading distance. Having the option to configure readers for the right opening mode, long range or tap, and to fine tune the optimal reading distance depending on the environment are important features of a carefully considered mobile access solution.

When implementing any new type of solution it is crucial to consider the impact it will have on users. First impressions are lasting ones and the solution may be easily dismissed if it does not meet expectations. The experience of opening doors with mobile devices must be streamlined, intuitive and convenient; the user should not be required to perform too many steps. If one has to unlock the device, start an App, select a Mobile ID and then present the device to the reader, the user will quickly find their current physical badge to be a better solution. It is also important that the user have an equally smooth experience on different mobile platforms; having one experience on Android and a different on iOS will result in confused employees and more training and support calls for the security staff.

Management considerations

Managing badges and identity cards can be a time-consuming task for security staff. University administrators have their own set of challenges when thousands of students show up in a short time frame at the beginning of the year. Ordering, printing, handing out and managing lost cards takes up valuable time for security personnel as well as employees and students.

The benefits of mobile access are not limited to the convenience of opening doors. Connected mobile devices introduce new possibilities to manage mobile identities in near real time. Using a cloud-based portal to centrally manage identities frees up time for staff, who today are managing physical badges.

A robust mobile identity management system has proven processes for managing employees and students, and the entire life cycle of mobile identities to increase the efficiency of security administrators.

A key feature to consider when implementing mobile access control is how an employee is on-boarded and issued a mobile identity. Simply adding a user's name and email should trigger the process to send out an invitation email to the employee with instructions on how to install the App. When the App is installed and configured the correct mobile identity should be provisioned to the mobile device and the security administrator should be notified when the process is complete. For larger organizations it should be possible to mass upload user data from a file. The mobile identity platform should validate the data and, for each user, go through the process of sending an invitation email, issuing an appropriate mobile identity, and notifying the security administrator when a user has installed the App and has been provisioned a key.

Mobile identities should be unique, and when ordered they should automatically be configured to match the specific attributes of the organization and the facilities where they will be used. Issuing a mobile identity to an employee or student should require only selecting the user and the correct mobile identity. Manually entering physical access control system (PACS) numbers and facility codes is prone to errors and is time-consuming which will likely result in a bad experience for the staff managing the mobile identities.

Many organizations have offices around the globe with different access control systems and an employee visiting a remote office is often required to get a visitor badge. With a mobile access solution supporting multiple mobile identities per mobile device, an employee can receive an additional mobile identity before leaving or upon arrival. As the iPad® and teablets become more common in the workplace, having the ability to connect an employee with different mobile devices will be another important feature.

Using a mobile device for logical access to authenticate to different services is a clear trend in the market. Many organizations today see the benefit of converging physical and logical access to cut costs and improve security. A common mobile identity platform for both physical and logical access makes it easier for security administrators to manage access rights and for employees to authenticate to different services as the mobile device will be a common platform. A security administrator can send out identities on-demand to a single employee or a group of employees; these can then be used for logical access to enable signing on to services such as VPN and email using strong authentication, all managed in one mobile identity platform.

Security considerations

Attacks can come from many directions, utilizing many tools and tactics. Protecting each link within a mobile access solution and ensuring that there is no single point of failure between readers, mobile devices and back-end security systems requires a multi-layered security model. In the rare event criminals succeed in breaching one layer, the doors beyond remain locked.

Managing digital keys on mobile devices requires a holistic view of end-to-end security, beginning with how the digital keys are generated, managed over their life cycle and stored on mobile phones. The mobile identity platform must be designed with security as the first priority, and all mobile identities and user information should be protected in a secure vault based on Hardware Security Models, where all encryptions keys are stored and used in cryptographic operations.

Modern mobile operating systems such as Android and iOS are built to maintain a high level of security and a mobile access App should be built to take advantage of the security features. The App should run in a dedicated Sandbox which ensures that no other Apps can access or modify data used by the App and sensitive data and keys shall be protected by a device keychain, an area on mobile devices used for storage of sensitive data. In addition to the security of the mobile OS, mobile identities shall be signed and encrypted to prevent any manipulation of the mobile identities.

As with physical cards, the ultimate control of who is allowed access to a building is decided by the local access control system. If a mobile device is lost, stolen or compromised the access rights for its digital credential can be inhibited in the access control system, preventing any unwanted access. In the unlikely event a mobile device is compromised, the attack should be limited to the specific mobile identities installed on the device, as each digital key should be unique. An employee is also far more likely to notice a lost mobile device than a physical badge.

Mobile devices also have an advantage over physical cards as they are on-line, if a security administrator wants to remove a digital key from a device, the mobile identity can be revoked over the air as long as the device is connected to the wireless network; if an employee reports a lost device, the mobile identities can be revoked before the device ends up in the wrong hands.

To further reduce the impact of a stolen device, mobile identities can be configured to only engage with readers when the mobile device is unlocked. This means that an unauthorized user would have to get around the device PIN, face recognition or fingerprint protection to be able to use it to open doors and access the building.

Considerations when implementing Mobile Access

When implementing mobile access there are a few things to consider before deciding on the type of reader to invest in. The installed base of mobile devices can affect the technology choice as iPhones 5s and earlier do not support NFC. In organizations with a large base of iPhones, Bluetooth Smart is the only option. The types of doors to be mobile-enabled should also be considered. Parking garages, main entrance doors and elevators can all benefit from a longer read range by increasing convenience for the employees. Areas where many readers are in close proximity to one another should utilize a tap experience to minimize risk of opening the wrong door; both NFC and Bluetooth Smart-enabled readers can support a tap experience.

Many organizations have a mobile device management platform where corporate Apps are published and run in a specific container on the mobile device. Making sure the mobile access solution is interoperable with the MDM platform can make sense especially if security settings are controlled by the MDM platform.

Leveraging existing investments in physical cards and readers should also be considered. Even though mobile access increases convenience, some organizations might allow their employees to keep the physical badge as a backup, while still promoting a seamless migration to a more secure standard and mobility.

Summary

As companies merge security and convenience at the door by transforming smartphones and other mobile devices into trusted, easy-to-use digital credentials that can replace keys and smart cards, there are certain things to consider when choosing a mobile access solution. To be certain the solution works with the latest smartphone technologies and is able to evolve with the mobile industry, it should be rooted in a standards-based card technology that can be emulated on a large number of mobile phones, tablets and wearables. To gain acceptance among employees and students, the user experience must be equal to that of physical cards.

First impressions last, and the solution may be easily dismissed if it does not meet expectations. The experience of opening doors with mobile devices must be streamlined, intuitive and convenient; the user should not be required to perform too many steps. An interesting value proposition of mobile access is the possibility of sending and revoking mobile identities in almost real time, and for maximum benefit, the mobile identity platform must be designed for administrator convenience and efficiency. Mobile access presents the opportunity to dramatically alter how we open doors and interact with our environment, and when implemented correctly, the future of access control will come knocking.

2014-10-16-2014-wp-en