What Do I Need to Know to Successfully Deploy Mobile Access?

Part 2

INTRODUCTION

Part 1 of our eBook series, “Mobile Access - What You Need to Know”, demonstrated the benefits of adopting a mobile access solution for your organisation. If you did not have the chance to read Part 1, you can access the download here:

Part 1: Mobile Access - What you Need to Know

In this part, we discuss what you need to know in preparation to deploy a mobile access solution.

Using a mobile device to gain access to buildings is not only about solving a particular problem; it’s also about doing things better.

Confidence and education in the use of contactless applications and technologies, such as Near Field Communications (NFC) and Bluetooth, are continuously growing. In the era of mobility and cloud computing, companies are increasingly concerned about the security and protection of their physical environment. Correctly implemented, mobile access has the potential to revolutionise the way we open doors.

With this in mind, we’ve produced this guide to mobile access configuration to help answer two critical questions:

- What are the underlying technologies which enable mobile access?
- What do I need to know to implement mobile access control?

1 What do I need to know about mobile access technologies?

COMMUNICATION STANDARDS

Currently, there are two communication standards that can be employed for mobile access: Near Field Communications (NFC) and Bluetooth Smart. Which standard you choose for your deployment is largely driven by what you need your solution to do.

Bluetooth Smart

Bluetooth Smart (also referred to as Bluetooth Low Energy [BLE]) is a relatively new wireless technology. Bluetooth Smart provides considerably reduced power consumption and lower implementation costs while maintaining a similar communication range.

Bluetooth Smart is now finding its way into the payment, home entertainment and security industries, among others. By 2018, more than 90 percent of Bluetooth-enabled smartphones are expected to be Smart Ready devices.[1]

- The longer read range of Bluetooth Smart can be read at distances up to 10 m.
- Readers may be placed on the secure side of the door or hidden away.
- Bluetooth Smart is supported on both Android and iOS devices.

Key Takeaway: Bluetooth Smart is able to operate both at close range and from a distance, supports both iOS and Android, and has low power consumption. Environments with mixed device populations and those that require activation from a distance are best served by this communication standard.

1 Bluetooth SIG, Mobile Telephony Market, accessed 10 August, 2015.

NFC

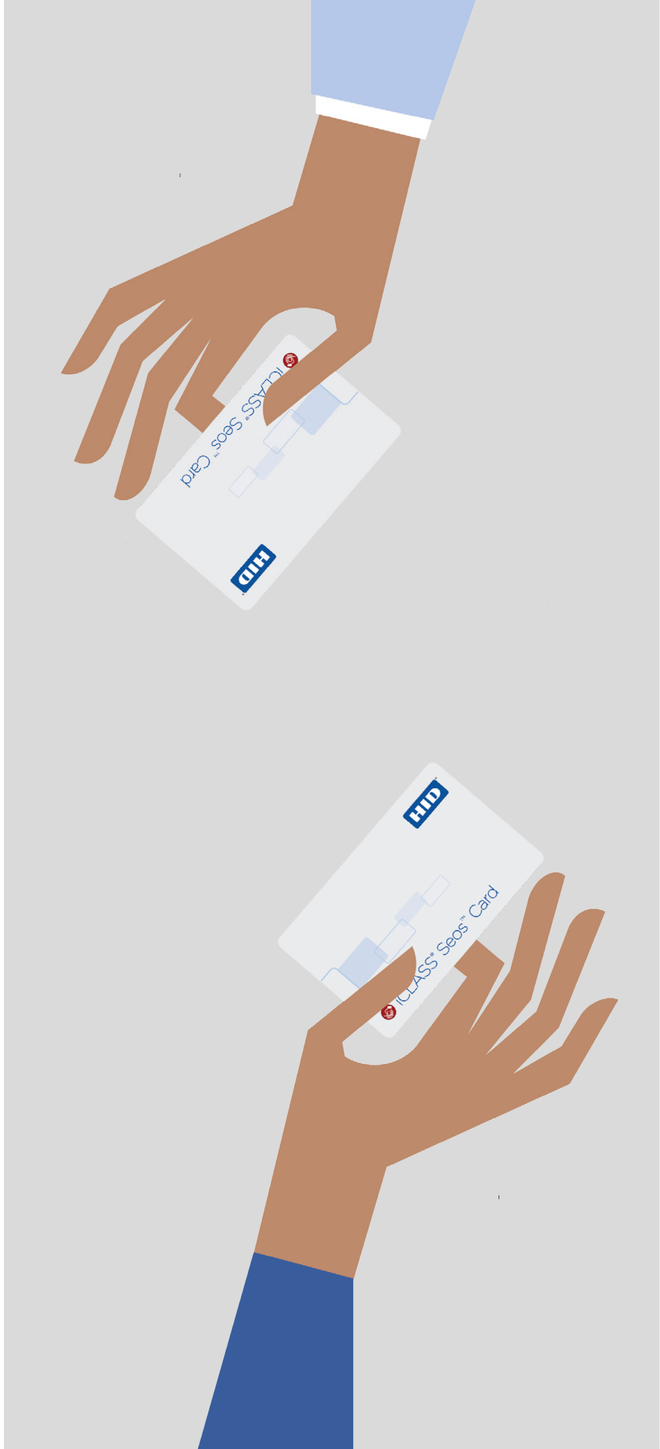
NFC is a wireless communication technology that enables smart devices (including embedded tags) to establish radio frequency communication with each other over very short distances (typically 10 cm or less).

The NFC standard supports four modes of operation:

- Reader/writer mode: Smart devices are capable of reading information stored on embedded NFC tags, labels, etc., over NFC.
- Peer-to-peer: Smart devices can exchange data over NFC.
- Card emulation: Smart devices can be used like a contactless smart card over NFC.
- Host card emulation: Software applications can emulate contactless credentials.

To date, iOS does not support the NFC standard.

Key Takeaway: The NFC standard, operating in HCE mode, is a good choice for close-range applications (less than 10 cm or direct contact with a “tap”) that do not include iOS devices in the mobile population.



NFC vs. Bluetooth Smart – Comparison Table

	NFC	Bluetooth Smart
Standardisation body	ISO/IEC	Bluetooth SIG
Radio frequency	13.56 MHz ISM	2.400 GHz – 2.4835 GHz ISM
Range	< 10 cm	> 10 m
Current consumption	< 15 mA (read)	< 15 mA (read and transmit)
Chip requires power	No	Yes
Over-the-air data rate	424 kbit/s	1 Mbit/s
Supported operating systems (for mobile access control applications)	Android 4.4 + BlackBerry 10 + Windows Phone 8.1 +	iOS 7 + Android 4.3 + BlackBerry 10 + Windows Phone 8.1 +
Storage of credentials	Encoded in device operating system (Host Card Emulation); can be further protected by Trusted Execution Environment or MDM systems	Encoded in device operating system; can be further protected by Trusted Execution Environment or MDM systems
Transaction experience	Tap	Tap Automatic (no action) Gestures
Common access control use cases	Standard (single doors) Locations with many doors nearby (e.g. conference centres) Combination of security factors (e.g. phone + PIN) When counting transactions is required	Standard (single doors) Long range (e.g. car park gates, garages) Hidden readers

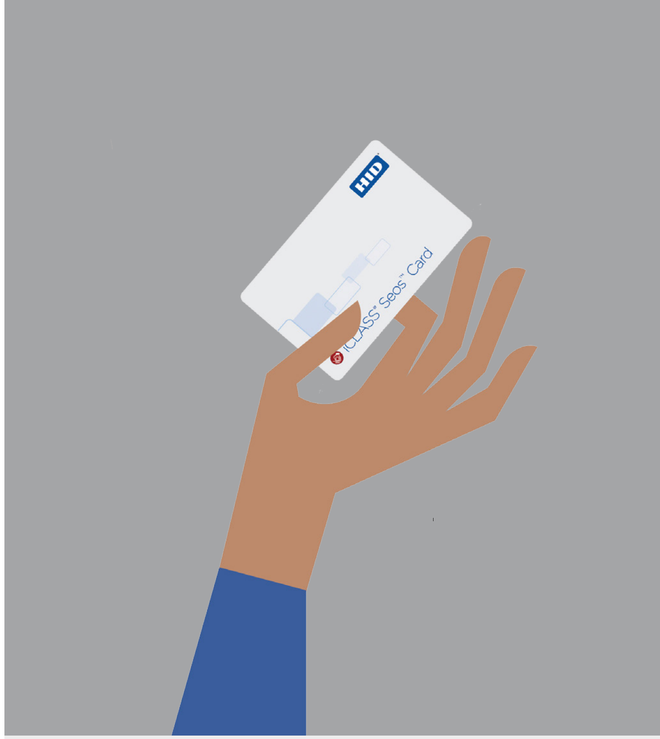
INFRASTRUCTURE

Mobile devices, readers and locks are part of an integrated infrastructure protected by security technologies, such as strong encryption and multi-layered authentication. These can be managed by a cloud-based portal application. The following is an overview of how these technologies connect.

Network Technologies

A relatively new concept is the Internet Area Network (IAN). This is defined as a communications network connecting voice and data endpoints within a cloud environment over Internet Protocol (IP). This concept eliminates older, more geographic references, such as local/wide area network (LAN/WAN), because it supports virtualised applications and services, no longer tied to physical locations.

Key Takeaway: The Internet Area Network (IAN) can support virtualised applications in the cloud. For mobile access applications, the IAN provides support for cloud-based operations.

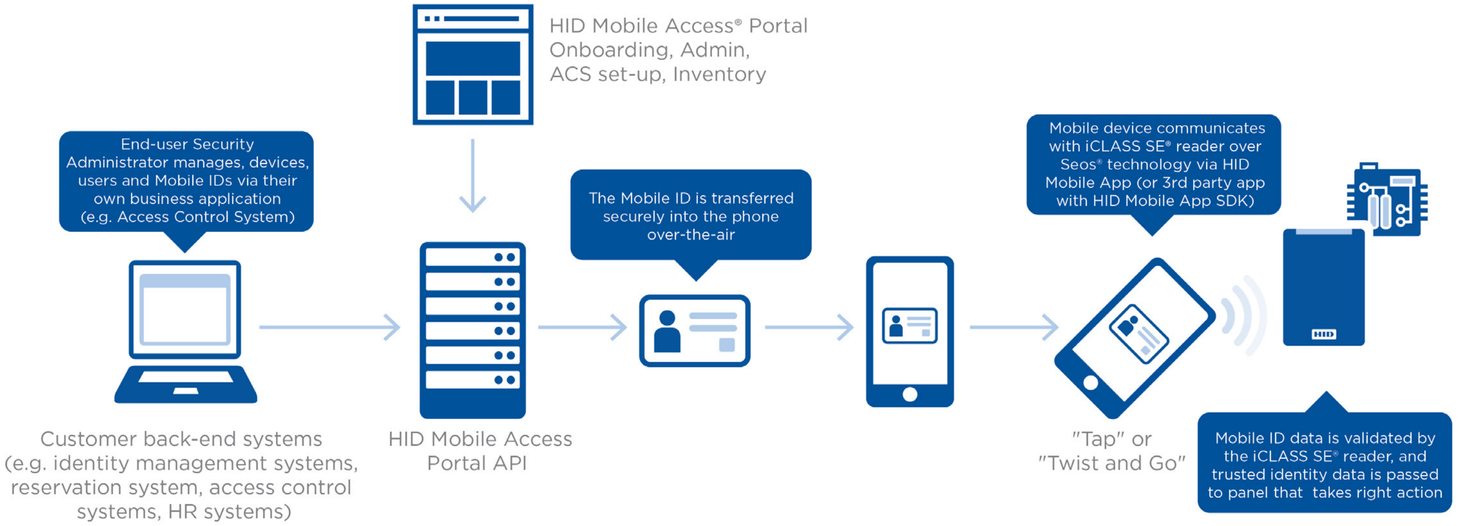


Portal Technologies

Client-side scripting enables developers to design user interfaces with the familiar behaviour of desktop operating systems. The combination of client-side scripting with server-side technologies provides even more flexibility, allowing administrators to remotely perform management, configuration, reporting or troubleshooting tasks in their web browsers over a secure network connection.

Application programming interfaces (API) allow integration of the portal with back-end systems. In the case of mobile access control, the management portal can be integrated with the company's access control system (ACS) and mobile device management (MDM/EMM) systems for seamless management of users and user groups, roles and access rights, identities and devices.

Key Takeaway: Portal technologies offer a user-friendly web experience for management and reporting functions. They also offer the added benefit of being able to connect to back-end systems, providing operational efficiencies and a seamless user experience.



Cloud Computing

Cloud computing is the access and use of (shared) computing resources (e.g. storage space, computing capacity, servers) “as a service” over a network. Cloud computing solutions provide the ability to store and process data in remotely located data centres, usually owned by third-party service providers. These services are accessed using local browser functions, defined interfaces and protocols.

The primary enabling technology for cloud computing is virtualisation. Virtualisation is the creation of virtual machines, logical desktops, servers or storage spaces that are separated from the underlying physical hardware and software. Virtual resources can be shared by several customers. Use is allocated according to demand, maximising efficiency.

A growing number of organisations are using cloud-based resources and applications for a variety of purposes. Much of this can be attributed to the expanding capacity and performance of broadband networks and computing hardware. Advantages include the following:

- Cost reductions (no need to buy and administrate hardware and software).
- Scalability.
- Location independence.
- Increased productivity through better collaboration.

Key Takeaway: Mobile access solutions that are accessed through the cloud offer operational efficiencies, such as being readily scalable and offering centralised management over multiple locations.

Security Technologies

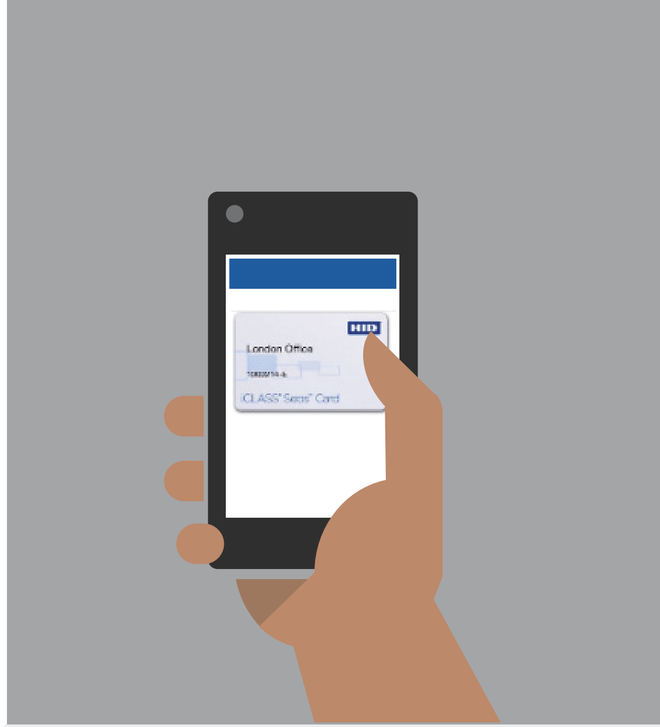
When using network and cloud resources to store, access and process critical data, security is paramount. Secure access to private (corporate) networks over an untrusted public network, such as the Internet, can be established through a virtual private network (VPN).

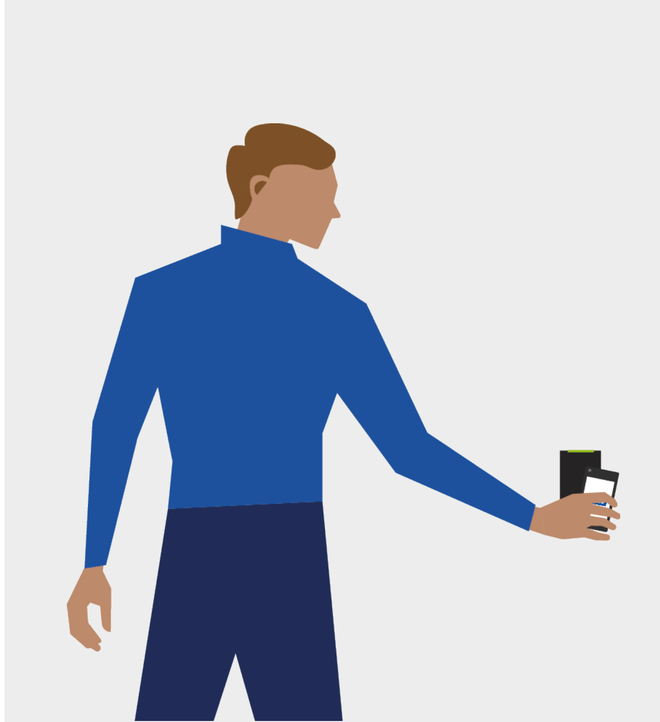
Encryption protects sensitive information by encoding it in such a way that a decryption key is needed to read data.

Encryption can only protect confidentiality of information, but not its authenticity. Therefore, another important security aspect and best practice is multi-layered authentication. Upon log-in, users should be required prove that they are indeed authorised users through a multi-layered authentication protocol.

More importantly, service providers must undertake appropriate measures to maintain application and data security, such as firewall and intrusion protection, high-security policies, server OS-hardening, security patch management, etc.

Key Takeaway: Mobile access solutions that follow best practice should employ multi-layered authentication protocols to protect sensitive identity information and unauthorised entry into the system.





2 What do I need to do to implement mobile access control?

SYSTEM ARCHITECTURE

When implementing mobile access control, the underlying architecture is comprised of more than mobile devices. It also consists of reader selection, transaction security, mobile app integration and potentially back-end integration.

Here are a few things to consider before deciding upon a particular technology:

- What access control scenarios need to be addressed?
- What role is mobile access control expected to play in these scenarios?
- Is the objective to combine the use of mobile devices and smart cards, or to transition to using only mobile devices?
- How do I ensure security, privacy and convenience for all access scenarios (access to doors, data and cloud applications)?
- How many users will the system serve?
- What different roles and access rights need to be assigned and managed?
- What new processes or policies need to be established?
- How can I integrate mobile access controls with our back-end systems?
- Is it feasible to integrate access control and credential management with mobile device management (MDM/EMM), directory services and other systems?
- What areas need to support mobile access: parking garages, main entrance doors, elevators, office doors etc?
- What communications standard(s) support the use cases I need to support?
- How is over-the-air-communication between server, mobile devices and readers secured?
- How can I ensure the investment in mobile can be leveraged well into the future?

The Mobile Environment

Deploying mobile access control requires a seamless, end-to-end system consisting of smart devices, Mobile IDs, readers, locks and services. Organisations implementing mobile access control should focus on the following areas of consideration:

Creating a secure mobile access environment

Quality mobile access control solutions handle secure identity through multi-layered authentication, thereby establishing the identity is real and validating that the identity data is coming from a trusted source.

Management of Mobile IDs

Mobile IDs should be created and managed by a centralised management platform. Transmission of sensitive identity data to both the access control system and the mobile device should ensure security and privacy in communication.

Multi-layered authentication for physical and logical access control

In contrast to form factors driven by low frequency legacy technologies, smart devices can increase overall security through multi-layered authentication.

Choosing readers and locks

Readers and locks must support the mobile access control solution you choose. In use cases where meeting compliance initiatives or requirements for enhanced privacy and protection are present, the ability for the solution to support these features must also be considered.

Provisioning Mobile IDs

Over-the-air transmission of Mobile IDs should be supported by an appropriate security infrastructure in order to create, issue and revoke lost or stolen credentials. The ability to monitor and modify security parameters should also be present in the management portal.

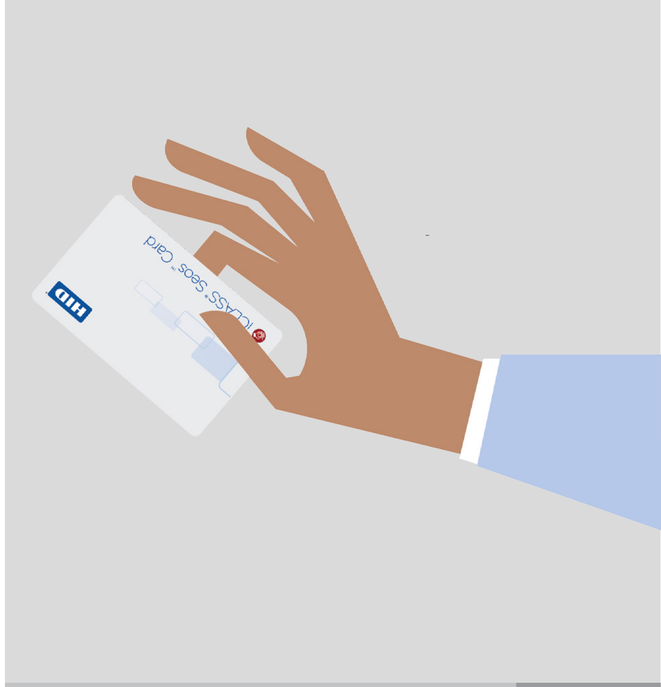
CONSIDERATIONS

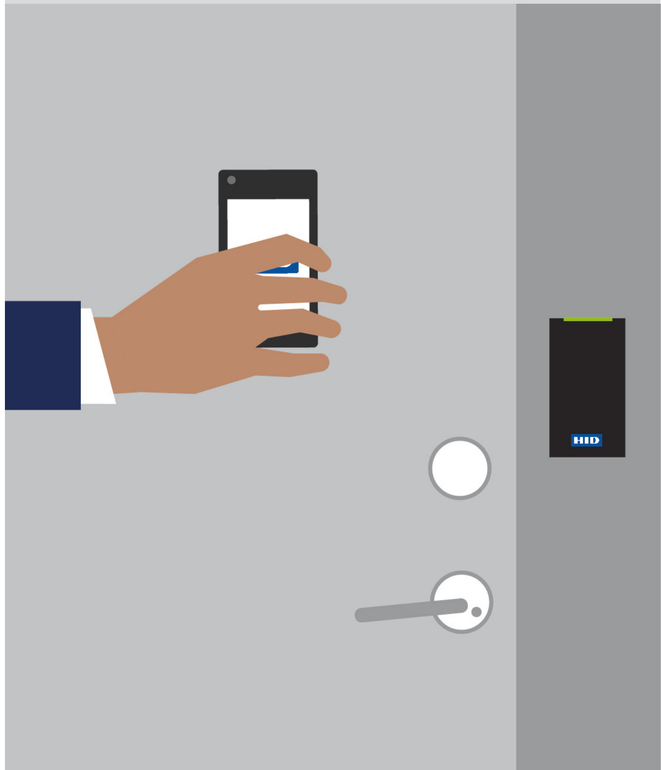
Management Considerations

How you manage Mobile IDs is dependent upon different factors:

- Scope (physical access only or a unified access solution).
- Users and roles.
- Security levels.
- Number of locations.
- Number of devices per user that need to be supported.

The management portal should support the entire lifecycle of the Mobile ID. Centralised, cloud-based management with secure over-the-air management of the Mobile ID is highly desirable. Management efficiencies are created through automatic configuration of mobile identities, batch upload of multiple user profiles and batch notification features.





Security Considerations

A mobile access solution should be designed with security as a first priority. Managing sensitive identity data on mobile devices requires a **holistic view of end-to-end security**: How are Mobile IDs generated? How are they managed over the entire lifecycle? How can Mobile IDs be securely stored on mobile phones? Attacks can come from many directions, utilising different tools and tactics.

Mobile IDs must be **encrypted** to prevent manipulation. All Mobile IDs and user information should be protected by cryptographic operations. Applications that manage Mobile IDs should run in a dedicated sandbox, ensuring no unauthorised apps can access or modify data. Best practice is to ban jail-broken or rooted devices from business use.

Just like physical cards, mobile devices can go missing. If a provisioned device is lost, stolen or compromised, access rights for the **Mobile ID should be easy to revoke**. If a device is found or replaced, it should be just as simple to provision again. Organisations should establish a reporting process as part of sound policy.

To further reduce the impact of a stolen device, devices can be configured to engage only with readers when the device is unlocked. As a matter of course, communication between the access control centre, management portal, mobile devices and readers must be protected. End-to-end encryption of **communications protects personal data and prevents cloning**. Best practice is to use trusted back-end services, working independently from the actual communication protocols being used.

Invitation codes used to authorise provisioning of Mobile IDs should also be protected through the use of **One-Time-Password (OTP) security**. It is also important to ensure your cloud-based management application is properly protected. **A multi-layered authentication approach is highly recommended**.

Mobile-enabled Readers

Readers must support your communication standard of choice. In cases where a gradual migration is desired, the **readers should be as interoperable as possible** to support a mixed population of access control technologies.

Reading distance is another important factor when implementing different mobile access control applications. Given the nature of contactless technologies, achievable reading distances can vary depending on the environment in which a reader is placed. The type of smart device used can also affect the reading distance. Having the **options of fine-tuning the reading distance** depending on the environment and configuring readers for the desired opening mode (long-range, tap or gesture-based motion) are important features as well.

User Experience

Companies adopting a mobile access control solution should focus strongly on user experience because **user experience and acceptance is critical for success**.

Whenever a new type of solution is implemented, it is crucial to carefully consider the impact it will have on users and their daily routines. In order to gain acceptance, a new mobile access control solution must provide a user experience superior to other form factors. **First impressions are lasting ones**.

The mobile access experience must be **streamlined, intuitive and, above all, convenient**. When implemented correctly, mobile solutions can bring the spirit of innovation to access control.

CONCLUSION

No matter what the technology, mobile devices offer an unparalleled way to change how we open doors. However, it is important to review which mobile-related technologies will allow your organisation to create the optimal access experience for your employees.

Enterprises should look at the following before implementing mobile access control:

- NFC is a good choice for close-range applications (less than 10 cm or direct contact with a “tap”).
- Bluetooth Smart operates both at close range and from a distance; it supports both iOS and Android.
- Mobile access solutions that are accessed through the cloud offer scalable and centralised management.
- Mobile access solutions should employ multi-layered authentication protocols to protect sensitive data.

If you have any questions or would like to request a call back from one of our Sales Advisors, please send us an email and we will be in touch.

CONTACT US

To learn more about mobile access and HID Global, please visit: hidglobal.com/solutions/mobile-access.

Missed Part 1: Mobile Access - What You Need to Know? Read it here

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

mobile-access-ebook-enterprise-part-2-en PLT-02887

An ASSA ABLOY Group brand