COPPERNIC
MOBILITY I CONNECTED DATA I ANALYTICS

White Paper

Extending Access Control Systems Using Mobile Devices: **A Modern Solution for Enhanced Security**

Date	September 17, 2024
Pages	4
Author	Rob Vandervecht
Reference	MKT 240208

1. INTRODUCTION TO PHYSICAL ACCESS CONTROL SYSTEMS

In today's rapidly evolving security landscape, businesses and organizations rely heavily on physical access control systems (PACS) to regulate and monitor access to their premises. These systems provide a crucial layer of security by ensuring that only authorized personnel are allowed entry to secure areas. At their core, PACS work by utilizing identification credentials—typically in the form of badges, cards, or biometrics—to grant or deny access at entry points such as doors, gates, and turnstiles.

Physical access control systems are used across various industries, including corporate offices, government facilities, healthcare institutions, educational campuses, and more. They play a vital role in safeguarding sensitive data, expensive equipment, and critical infrastructure. For businesses, access control systems mitigate the risks of unauthorized access, theft, and potential damage to property. As physical threats and security breaches continue to evolve, PACS have become an indispensable tool for organizations that prioritize the safety of their personnel, property, and intellectual assets.

However, despite their importance, traditional PACS have limitations. They are typically fixed in place, meaning that access control is often confined to entry points where card readers and biometric scanners are installed. This restricts the flexibility of businesses in managing access in areas away from their main premises, such as remote sites, temporary locations, or large open campuses. In today's fast-paced and decentralized working environments, there is an increasing need for access control systems that are more mobile and adaptable.

2. EXTENDING ACCESS CONTROL SYSTEMS WITH MOBILE DEVICES

With advancements in technology, businesses are now able to extend their access control systems by using mobile devices that are capable of reading ID cards. This shift introduces the concept of mobile readers, which can operate away from buildings and fixed infrastructure. Mobile access control devices allow security personnel to perform access checks at virtually any location, without needing to rely on fixed readers or traditional access control setups.

Mobile devices, such as specialized handheld terminals, can be equipped with the necessary technology to read RFID badges—an essential feature that is lacking in standard consumer cell phones. While most consumer smartphones are equipped with near-field communication (NFC) technology, they are not designed to support the more sophisticated RFID protocols used by popular access control systems. This limitation means that businesses looking to enable mobile access control must invest in specialized handheld terminals that are purpose-built for security applications.

For example, handheld terminals from suppliers like Coppernic are equipped with the required RFID capabilities to read ID badges issued by leading access control system providers. These devices can also connect to wireless networks, enabling real-time communication with access control servers and providing a seamless extension of the traditional PACS infrastructure.

3. USE CASES AND BENEFITS OF MOBILE ACCESS CONTROL SYSTEMS

Extending access control systems using mobile devices opens up a wide range of use cases that provide significant advantages for businesses. Below are some key applications of mobile access control, each of which can deliver considerable benefits in terms of security, convenience, and cost savings.

3.1. Mustering

In the event of an emergency evacuation, such as a fire or natural disaster, it is critical for businesses to account for all employees, contractors, and guests. Mobile devices enabled for access control can facilitate this process through a practice known as mustering. Using mobile devices, security personnel can conduct roll calls away from fixed access points, ensuring that everyone present is accounted for.

In a mustering scenario, mobile readers allow security staff to scan ID cards and check attendance in real time, even in outdoor or remote locations. This rapid identification process helps ensure the safety of all personnel by providing a clear record of who has been evacuated. From a financial perspective, this use case often provides a strong return on investment (ROI), as the ability to conduct effective emergency evacuations can save lives and minimize legal liabilities.

3.2. Remote Access Points

Another valuable application of mobile access control is the ability to perform entry and exit checks at remote access points where fixed readers are impractical or impossible to install. This is particularly relevant for businesses with large campuse s, warehouses, temporary storage areas, or gated yards.

For instance, a business might have a storage facility in a remote location that lacks traditional access control infrastruct ure. Using mobile access control devices, security personnel can manage access at these sites by scanning ID cards and verifying access rights on the spot. This flexibility ensures that security is maintained even in areas where it would be too costly or challenging to install permanent infrastructure.

3.3. Security Tours and Inspections

Mobile devices also offer enhanced capabilities for security personnel conducting tours and inspections. Security guards can use mobile access control readers to check the identity and access rights of individuals they encounter anywhere within the facility. This real-time verification improves security by enabling guards to detect unauthorized individuals or suspicious behavior as they patrol the premises.

In addition to verifying access rights, mobile devices can also be used to record incidents or other observations made during the security tour. These records can be transmitted back to the central access control system for reporting and follow-up, further enhancing the overall security posture of the business.

3.4. Special Events, Field Trips, and Temporary Facilities

Mobile access control is particularly useful for special events, field trips, and temporary office facilities. When businesses organize events at off-site locations, they often need to maintain the same level of security as they would at their main premises. Mobile devices can be used to check the security status and attendance of participants, ensuring that only authorized individuals are present.

For example, during a corporate retreat or off-site training event, mobile access control devices can be used to scan attendee badges and monitor access to restricted areas. Similarly, mobile readers can be deployed on shuttle buses or other forms of transportation to ensure that all passengers are accounted for and authorized to participate in the event.

3.5. Visitor and Incident Data Recording

Since mobile access control devices are equipped with screen input capabilities and cameras, they can be used to capture and record a wide range of data beyond simple access checks. For instance, security personnel can use these devices to register visitor information, log incidents, and generate reports on security events. This data can then be synchronized with the central access control system for analysis and record-keeping.

The ability to capture visitor and incident data in the field is a valuable feature for businesses that need to maintain comprehensive security records. Whether it’s documenting a security breach, logging maintenance activities, or tracking guest visits, mobile devices provide a convenient and efficient way to collect this information in real time.

4. INTEGRATION WITH EXISTING SYSTEMS

Some access control providers have begun to offer mobile functionality as part of their existing offerings, recognizing the growing demand for flexibility and mobility in security solutions. However, even if a business's current access control system does not natively support mobile devices, this functionality can often be achieved through third-party software integrations.

For example, CopperAccess from Coppernic is a third-party solution that enables mobile access control by integrating with existing systems. This type of integration allows businesses to extend their current access control capabilities without having to overhaul their entire infrastructure. The result is a cost-effective and scalable solution that enhances security while maintaining the flexibility to adapt to changing needs.

CONCLUSION

As businesses continue to face evolving security challenges, the need for flexible and mobile access control systems has become more apparent. By extending traditional PACS with mobile devices, organizations can manage access in remote locations, enhance emergency response procedures, and improve overall security efficiency. Specialized handheld terminals equipped with RFID technology offer a practical solution for businesses looking to bridge the gap between fixed and mobile access control.

With use cases ranging from mustering and remote access points to security inspections and special events, mobile access control devices provide significant benefits that justify the investment in specialized equipment. As more businesses recognize the advantages of this approach, mobile-enabled access control systems are set to become an essential component of modern security strategies.

For more information on Mobile Access Control solutions, visit :
https://www.coppernic.fr/en/mobile-access-control/