



Mobile Access - What You Need To Know

Part 1

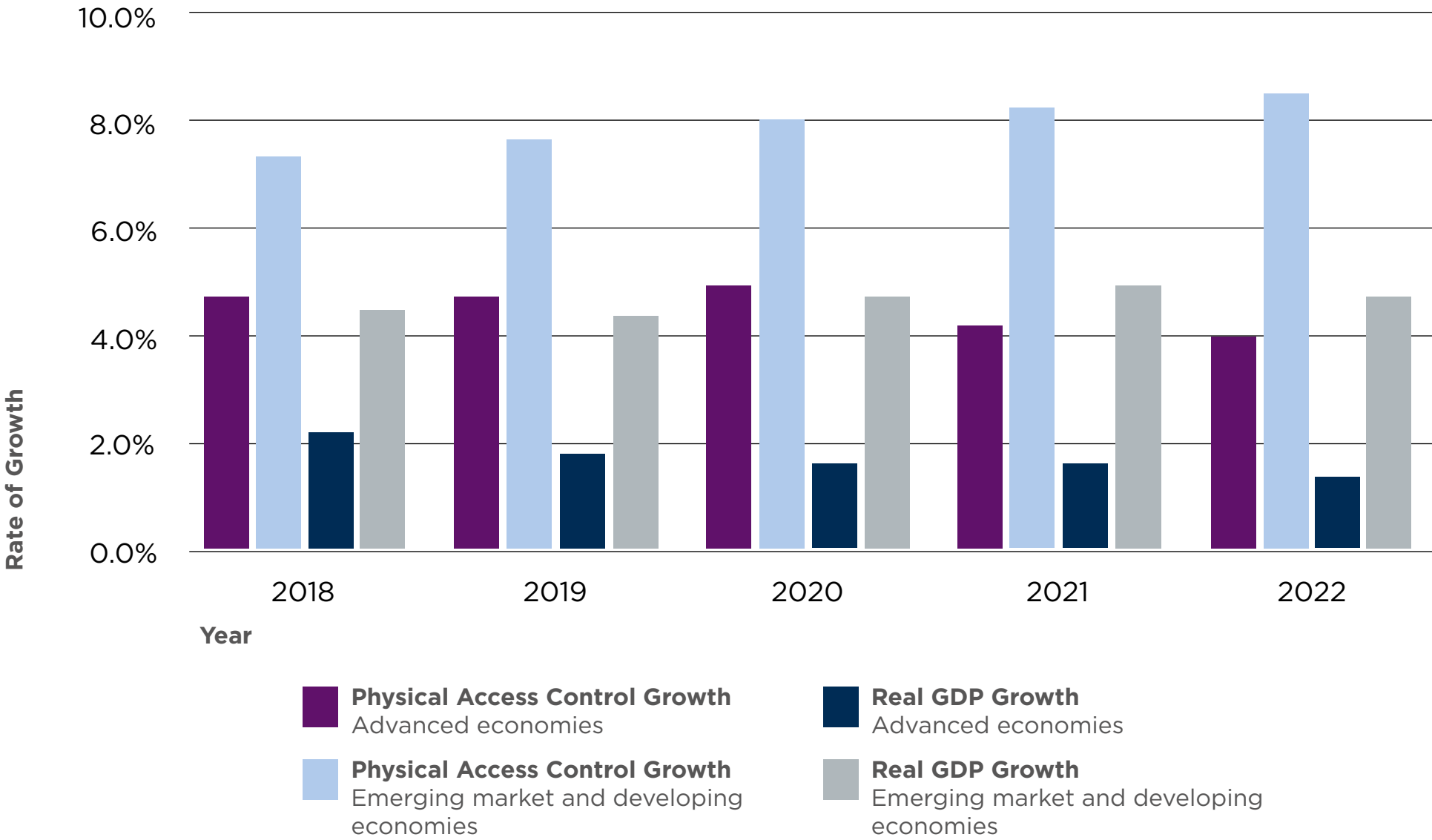
1 Why consider mobile access?

Despite the well-deserved attention paid to cybercrime and electronic data breaches, physical access control — restricting who can enter office space, data centers, and more — remains a critical frontline defense for organizations across industries and company sizes. Smart cards, key fobs and numerous other form factor technologies are commonplace in many office environments, and have been for some time.

Mobile devices are also ever-present in today’s office environment. These devices serve a number of purposes to their users: enabling communications in several forms, providing access to data and applications that previously required more cumbersome devices, assisting in locating available meeting rooms, cashless vending and efficient connectivity.

In light of these developments, using a smart device for controlling physical access (what the industry calls “mobile access control”) is a logical step for both employees and enterprises. This eBook will focus on the benefits of mobile access control in the new mobile-first world, help you understand the technologies that are available, and discuss what organizations need to consider when implementing a mobile access control solution.

The Rise of Mobile Identities Linked to Global Access Control and GDP Growth



- Physical Access Control Market Growth - IHS Access Control Intelligence Service
- Real GDP Growth Forecasts - IMF

2 Smart devices are everywhere

In 2018 the number of smartphone users reached three billion. Of those, the most popular smartphone brands are Samsung and Apple, with market shares of 27 percent and 24 percent, respectively.

Worldwide, it was predicted that by the end of 2018, about 39 percent of the population will be using a smartphone. That percentage is expected to grow to 48 percent by 2021.

North America has about 77 percent smartphone penetration, followed by 75 percent for Western Europe. Eastern Europe has about 60 percent, and the Middle East and Africa have the lowest smartphone penetration, with 19.9 percent.¹

The rising popularity of 'smart wearables' is also increasing the number of mobile devices in the market. These include glasses, clothing, fitness trackers, hearables and watches - which hold the major share.

Mordor Intelligence predicts the global market will register a CAGR of 19.1% from 2019 to 2024.² It is also estimated that a quarter of US adults will use a wearable device at least once a month in 2019. These truly mobile, "always-on" devices are even more natural candidates for access control applications because of the ready-to-use convenience of a wearable device.

1. newzoo.com - Global Mobile Market Report (2018)

2. mordorintelligence.com - Smart Wearable Market - Growth, Trends and Forecast (2019-2024)



3 What does HID Mobile Access[®] consist of?



End user administrator manages users and Mobile IDs via the HID Origo™ Management portal

Mobile ID is transferred to phone over the air

Reader is activated through a close proximity "Tap" or longer distance "Twist and Go" experience

Reader sends credential data to panel

Customer accesses control system

4 Enterprises expect a mobile-first world

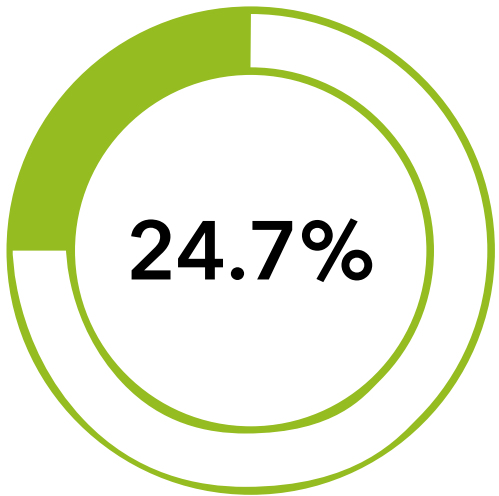
Driven by convenience and operational efficiency, enterprises are increasingly seeking to leverage the potential of a mobile-first world. Harnessing the mobile revolution for physical access control will eventually merge the network and other secure access needs, creating a more connected environment.

Enterprise mobility is not without its challenges, however. The “bring your own device” (BYOD) trend developed quickly and caught some enterprises by surprise. But BYOD challenges are gradually being met by more manageable methods of deploying mobile devices in the organization. Instead of an unknown, potentially unsupported population of employee-owned devices, organizations are granting select personal devices permission to access corporate systems.³ Several options, including the “choose your own device” (CYOD) strategy — where the organization offers a list of permitted devices and applications for specific roles — are overcoming these challenges.⁴

Extending physical access security to mobile devices increases enterprise efficiency by automating and eliminating a number of manual tasks. Consider how it changes a scenario that plays out in buildings all over the world each day.

³ [transparencymarketresearch.com](https://www.transparencymarketresearch.com) - Enterprise Mobility Market - Global Industry Analysis (2015-2022)

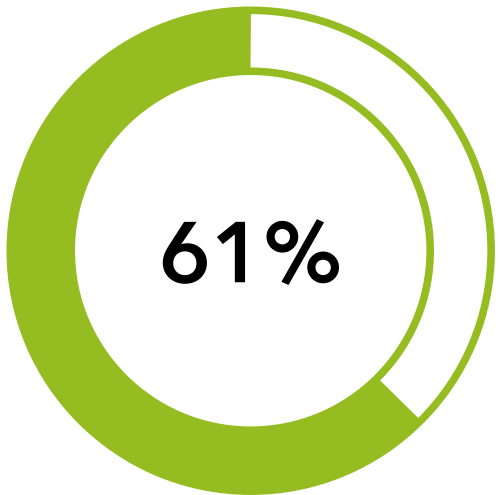
⁴ Adobe, 2016



Global enterprise mobility market
CAGR growth 2015-2022: 24.7%



Global BYOD and Enterprise Mobility
market growth 2014-2022: from
\$86 billion USD to \$510 billion USD³



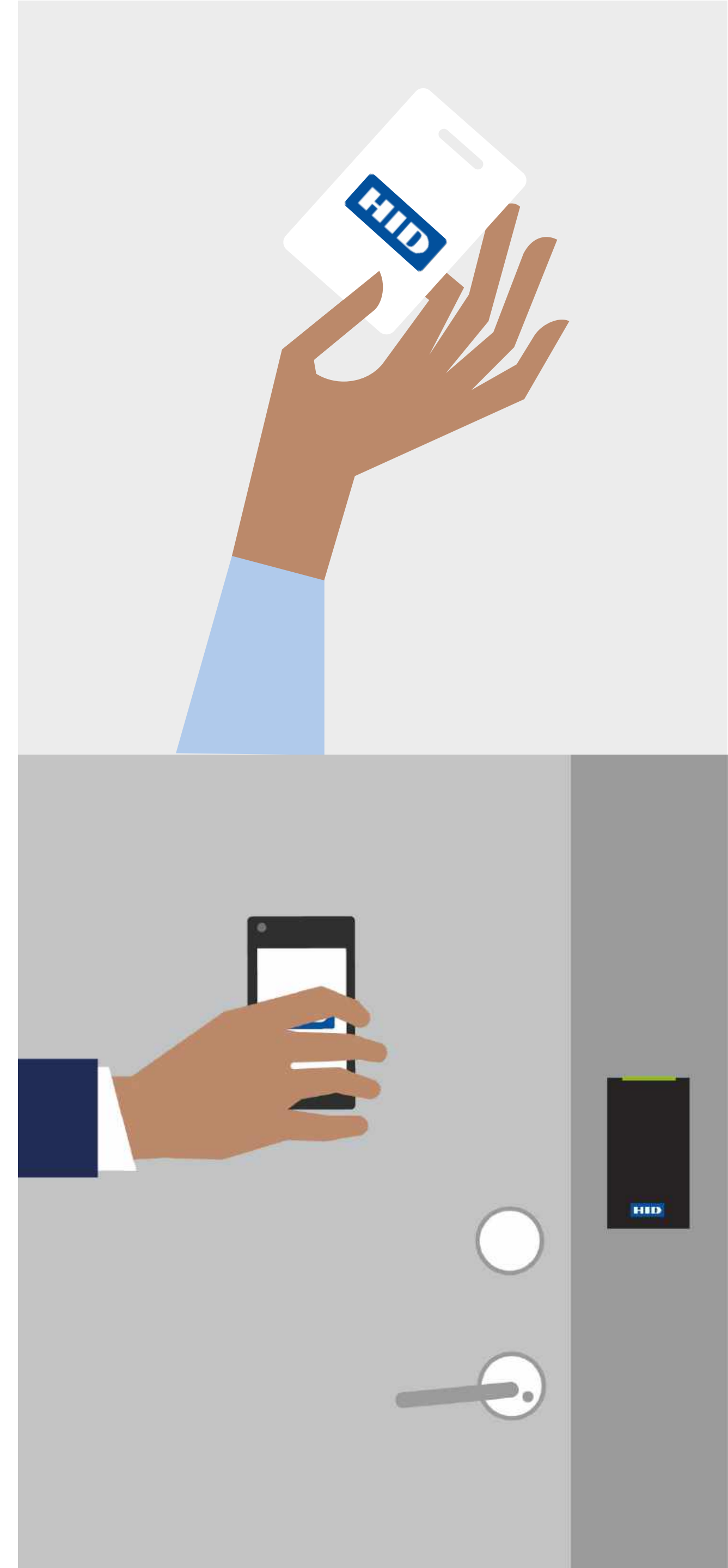
61% believe that organizations that
don’t deploy enterprise mobile apps
are at a competitive disadvantage⁴

5 The benefits of mobile access

A better, more convenient end-user experience

The freedom to move access control to phones, tablets, wristbands, watches and other wearables offers choice and convenience to end users, along with new and more convenient ways to open doors and gates.

- The smart mobile device is always on hand. Users do not have to maintain and carry multiple cards.
- Access with a mobile device can offer a quicker and smoother experience. In parking garages or at driveway gates, for example, the longer reach of the Bluetooth Smart communications standard makes it possible to drive up to the gate without having to roll down the car window and reach out to activate a reader.
- Smart device sensors, most notably the gyroscope and accelerometer, enable gesture detection. This offers an additional benefit for access control: the ability to open doors from a distance by performing intuitive gestures. For example, HID Global's patented "Twist and Go" technology allows users to unlock doors or open gates by rotating their smartphone in a way similar to turning a key. This also provides an additional layer of authentication for added security.

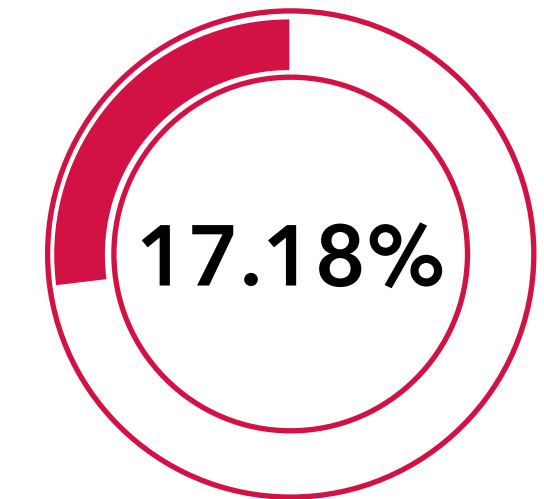


Mobile access can be more efficient to manage

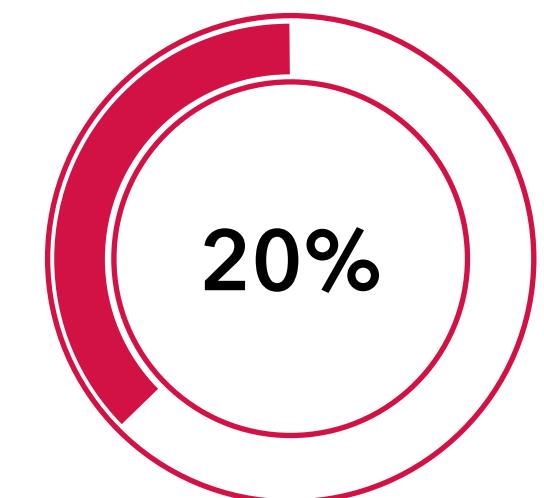
Connected mobile devices introduce new ways to manage mobile identities in near real time.

- **Time savings:** Using a cloud-based portal to centrally manage mobile identities frees up time for staff. It is even possible to enroll many users at once by importing a CSV or Excel file (batch upload). Invitations and provisioning to end users can also be managed via email.
- **Simple enrollment for end users:** An end-user receives the invitation via email, downloads the app, and enrolls. The Mobile ID is provisioned right to the end user's smart device.
- **Management of multiple locations:** Many organizations have offices around the globe with different access control systems. Employees visiting a remote office are often required to get a visitor badge. With a mobile access solution supporting multiple mobile identities per mobile device, an employee can simply receive an additional mobile identity on their phone before leaving or upon arrival.

Given the growing importance of cloud-based access control solutions, mobile access control portals will also provide great benefits to the Access Control as a Service (ACaaS) business model. ACaaS provides basic access control system functions to end users for a monthly subscription fee. The software usually resides on a server in the service provider's data center and can be accessed via a Web browser.



Global ACaaS service market valued at USD 764.8 million in 2017 and expected to reach USD 1.9 billion in 2023, a CAGR of 17.18%.⁵



20% of the current installed base of access control readers will be mobile capable by 2022.⁶

⁵ Market Research Future Report - Global Forecast (May 2019)

⁶ IHS Markit ACaaS Market Insight 2018

Mobile access can be more secure

Mobile access complements existing access control solutions by enabling the use of a smart device as an alternative to more traditional form factors. Smartphones or other smart devices provide a number of security benefits over smart cards or fobs:

- The PIN numbers used by keypad systems are easily shared. Legacy systems such as Magstripe and low-frequency proximity cards are vulnerable to cloning (record and replay).
- In quality mobile access solutions, digital credentials or Mobile IDs are securely stored and protected, utilizing the security features of the mobile operating system (e.g. sandbox or PIN) and strong encryption.
- Communication between device and reader transmits data over-the-air through secure communication protocols and trusted back-end services, independent of communication technologies such as NFC or Bluetooth.
- Because smart devices can communicate with readers over longer distances, the readers can be mounted on the safe side of a door, minimizing the risk of theft, physical attacks or observation.
- Cards and badges are much easier to lose than smartphones. Mobile phones are rarely shared or stolen in a working environment - something which happens more easily with cards.
- In the event of a lost, stolen or compromised mobile device, Mobile IDs can easily be revoked for all access rights remotely through the management portal.
- Smart devices also support multi-factor authentication, biometric identification and other advanced security features that extend far beyond the capabilities of legacy cards.



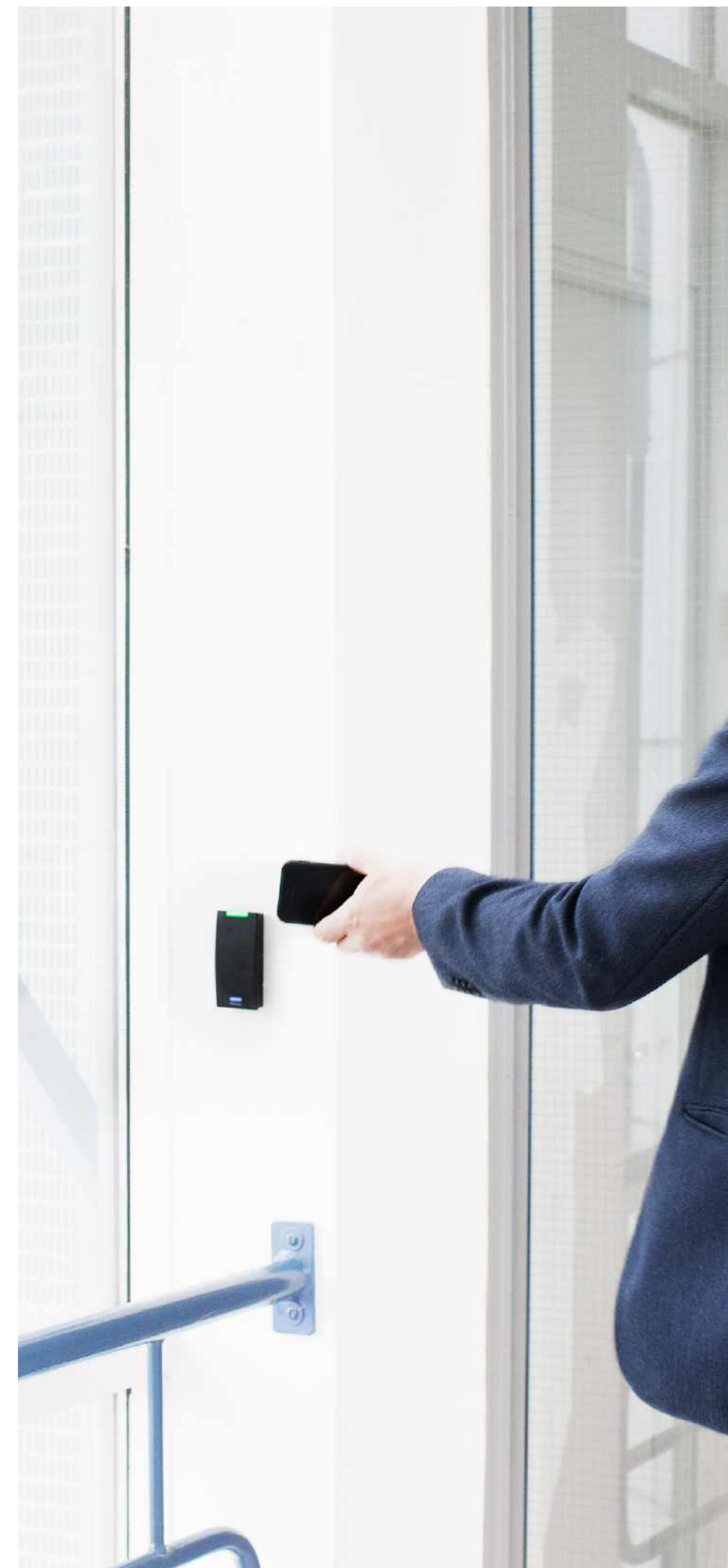
Mobile access enables a more connected environment

Today's organizations are beginning to see the benefit of merging physical and logical access. Simplified management, reduced expenses of maintaining multiple systems, improved security and enhanced user experience are driving this trend.

Smart devices can deliver additional security options for accessing data networks by enabling multi-factor authentication. They can generate other security features, such as the one-time passwords required for accessing the network or web-based applications.

Employees can conveniently use the same device for building access, VPN authentication and wireless network access, as well as for logging into the corporate intranet, email server, cloud-based applications, single-sign-on clients and other IT resources.

A shared mobile identity platform for both physical and logical access has several benefits. It makes it easier for security administrators to manage access rights, reduces errors resulting from improper synchronization between two separate management systems and offers greater convenience for employees to authenticate to different services.



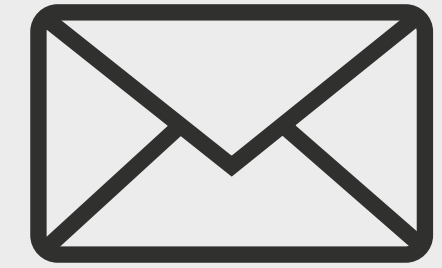
6 Conclusion

Mobile devices are changing the way that workers and enterprises think about their operations, networks and security. The logical next step for many organizations is replacing legacy systems for future-proof and flexible physical access control solutions supporting mobile access.

- Putting mobile devices to work as tools for secure access is more convenient for users.
- Easier for enterprises to manage; more secure than previous-generation technologies.
- Creates opportunities for the convergence of network and physical security that are simply unavailable with legacy access tools.

To learn more about HID Mobile Access and request a free consultation, click [here](#).

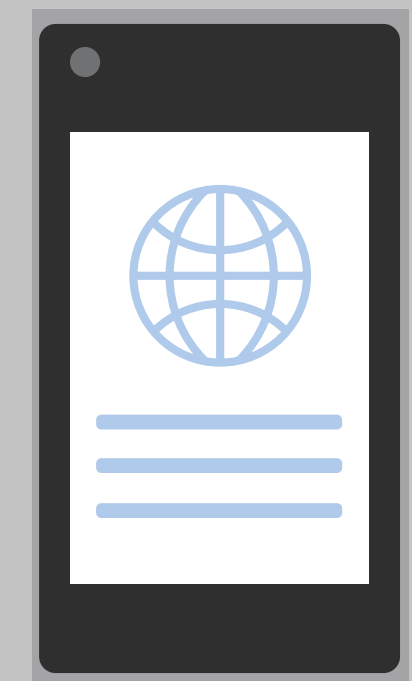
Read more in Part 2: What Do I Need to Know to Successfully Deploy Mobile Access?



Send



Download



Enroll





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

© 2019 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design and HID, the HID logo, iCLASS SE, Seos, iCLASS and HID Mobile Access are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2019-05-28-pacs-mobile-access-eb-enterprise-pa rt-1-en PLT-02886

An ASSA ABLOY Group brand

ASSA ABLOY