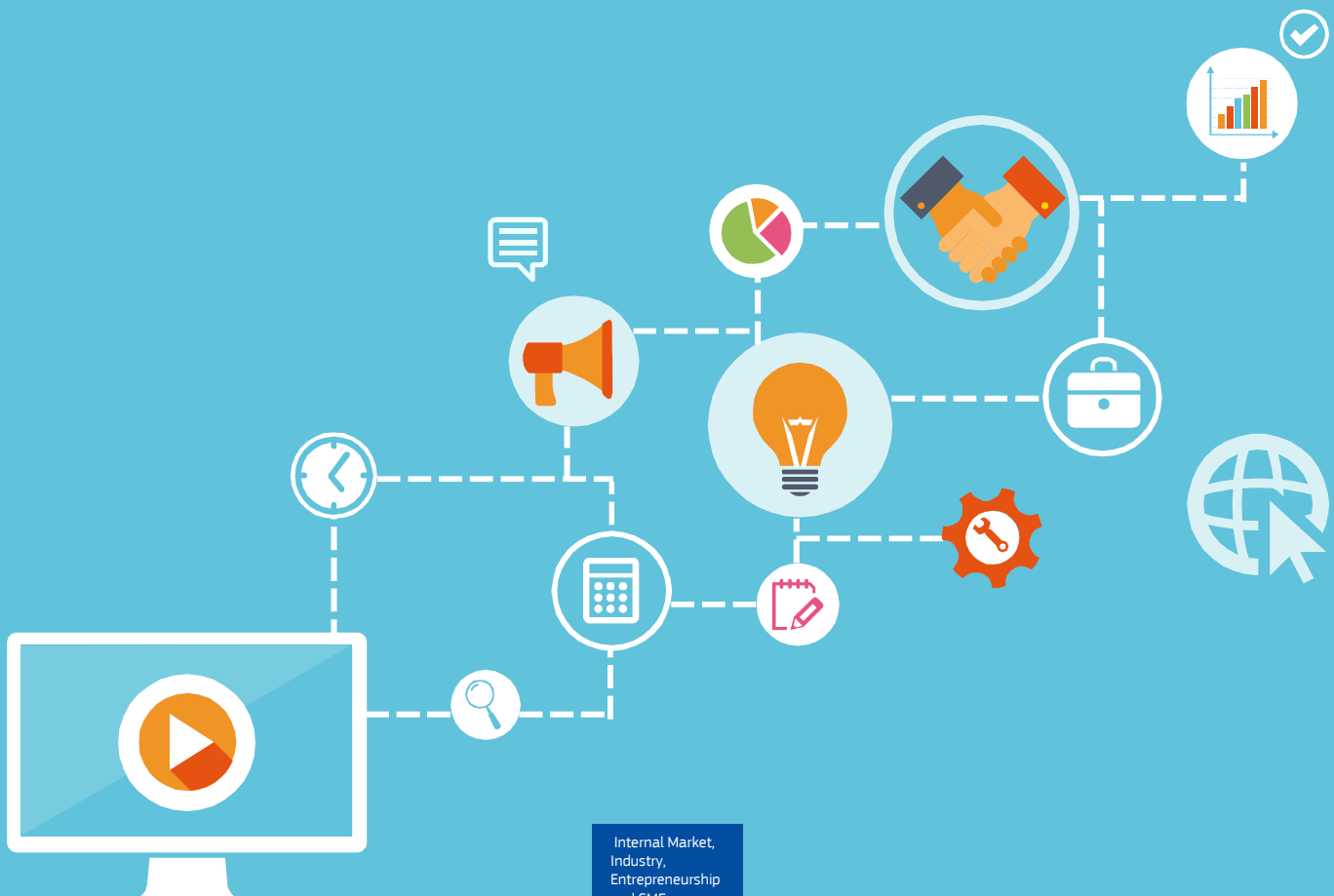
European Commission

Digital Transformation Monitor

Secure access control: Smart ID Management for building access

October 2017



Internal Market, Industry, Entrepreneurship and SMEs

© Mikko Lemola/Shutterstock.com

Secure access control: Smart ID Management for building access

Physical access control is an industry which is moving slowly in terms of change but the introduction of technologies like smartphones, wearables and biometrics seems to seduce specific sectors. Hospitality, healthcare and banks are attracted by those solutions meeting with their requirements. Growing security concerns and increasing adoption of technologies can encourage the market for a smarter and better security access control.

1

Security remains a strong concern

Secure access control can be defined as a system capable of identifying who enters or leaves an area of control and managing the admittance of the person to the building, a specific space or site.

Different factors for access control

Access control is one segment of the physical security equipment and services. In terms of access control specifically, the segmentation of the market is defined by type of reader technologies.

Actually, access control covers a broad scope of solutions with different factors that can be broken down into four categories as follows:

- Mechanical keys, entryphones
- Touchpads and keypads for entering password or PIN
- Multitude of types of cards such as magnetic strips, proximity cards, smart cards, photo-ID badges
- Biometric systems comprising fingerprint, palm, iris, face recognition

Those solutions vary in level of security, price and power consumption requirements.

Market size

According to IHS Markit research, the access control market was estimated at 4.2 billion USD in 2017[1]. It is forecasted to keep growing and is expected to reach USD 9.80 billion by 2022[2].

Cards are still leading the market of physical access control

Today, card systems including NFC and RFID are the most used way to access buildings and clearly lead the market. Often those cards or badges are also used for other applications than accessing buildings, like identity verification, method payment for canteen or vending machines or even accessing specific equipment or information systems.

The Freedonia Group and Security Industry Association have conducted a study[3] in 2014 revealing that card-based systems contributed to 71% of the electronic access control demand followed by biometric systems which gain traction with 18%. Touchpads and keypads are in a declining trend.

Traditional providers

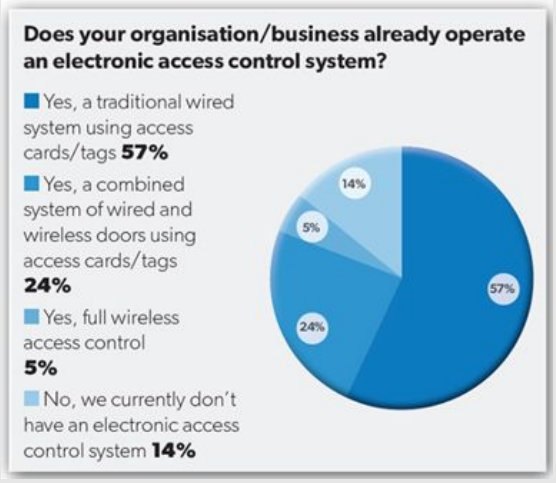
In the access control market, established players generally operate at international level with well-known brands. The major players include Bosch, Siemens, Honeywell, Assa Abloy and Tyco. Assa Abloy has acquired the technology HID Global.

Top 10 security access control providers

1. Honeywell Security (US)
2. Bosch Security (Germany)
3. Safran Security (France)
4. Assa Abloy (Sweden)
5. Tyco (USA)
6. Axis (Sweden)
7. Allegion (USA)
8. Aiphone (Japan)
9. TKH Group (Netherlands)
10. Avigilon (Canada)

source : asmag[5] based on 2014 revenue

Figure 1: Adoption of electronic access control system



Source : IFSEC[4]

2

Mobile technologies for greater security

Increased interest in the usage of smartphones as secure access control system

As smartphones have become ubiquitous in today's society, industries are aware of the smartphone's potential to be disruptive for secure access control by replacing current PIN systems, cards and keys. Indeed, the inclusion of NFC and Bluetooth technology on smartphones provides an industry-standard for exchanging access control data so users can present mobile credentials carried on their phones to a control access reader.

Use of smartphones for better ID management

The use of smartphones can notably eliminate the challenges and liability associated with the loss or omission of the PIN code, card or key. Using a personal item - difficult to lend to other people - especially a mobile device for secure access could add further security compared to the cards that are easily shareable. Users always bring them and are not likely to leave them behind. Also, they provide extra security layers thanks to biometric authentication of mobile phones or PIN keys required to unlock the device.

According to Allegion, a company specialised on security, it will also be a question of generation. When the current young generation who almost all carry a smartphone will enter the workforce, it will become more and more natural to migrate away from card-based systems.

What if the devices get lost ?

68 minutes to report a lost or stolen phone

26 hours to report a lost wallet with cards

Source: Unisys[6]

Low take off despite strong potential

There is a clear potential of replacement of traditional badges access with the use of mobile devices. Already in 2011, according to Avisian survey[7], over 70% of the end user community and 80% of industry respondents estimated a growing trend for additional credential form like phones, key fobs or tokens.

Today, few mobile apps are being developed to use and manage digital credentials in a secure way. However, the market for mobile access control remains immature today.

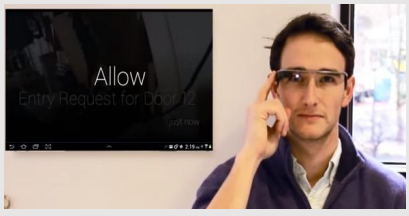
Development of wearables

The use of wearables can be also substituted in the same vein as the smartphone. Rings, wristbands and glasses have notably been developed, but are not very widespread.

Hotels and resort clubs are the biggest group of users of wristbands allowing their guests to access hotel rooms and authorised areas and use it for payments. Disney invested 1 billion USD in 2014 in the development of its own wristband called Magic Band. Today, all Disney resort hotels are equipped representing over 14 million guests using the wristband each year.

Brivo Labs, a company specialised in access control is working on wearable technology. The company has developed OKDoor, based on the utilisation of the Google Glass to allow or deny the access control.

OKDoor glass by Brivo Labs



Further authentication with biometrics

Designed for high security areas, biometrics associated with devices is becoming a standard requirement for secure access control delivering greater security as devices are not transferable, because the authentication identification on devices is based on a unique signature. Indeed, Multi-Factor Authentication (combination of different factors, typically cards or mobile devices with biometrics) is gaining importance, mainly targeting employees allowed to enter in critical areas.

Figure 2: Existing mobile applications for physical access control

Mobile application	Developer/Manufacturer	Deployment level
Twist and Go	HID Global	Tested in Netflix and Good Technology facilities in 2015
C-Cure Go	Tyco	Between 1 000 and 5 000 downloads
VIZpin	ECkey	Between 1 000 and 5 000 downloads
aptiQmobile	Allegion	Between 1 000 and 5 000 downloads
Digital Key	Hilton	1000 hotels in March 2017, expected 2500 by end of 2017
Hyatt Mobile Entry	Hyatt	Exclusively at Grand Hyatt San Francisco, Hyatt Regency Bellevue and now the Hyatt Regency Savannah.

Limited development of Multi-Factor Authentication

Few companies have developed secure access products combining smartwatch or wristband associated with biometrics to bring more security :

- Ionosys, a French start-up, has designed a smartwatch which can be activated with the owner's data biometrics: fingerprint, palm vein patterns or pulse. Ionoki has been tested in a sewage treatment plant facilitating the entrance to secured areas and also to allow access to specific applications. As end of 2016, 200 smartwatches have been ordered.
- Iritech, a specialist in biometrics technology, provides a solution using iris detection technology. The wearable is preloaded with user logins and passwords and then scanned to gain access to secured sites, computers, smartphones or tablets by matching iris capture with iris registration. The idea is to give, in a single device, all logins, passwords and codes of a user's daily life. A heartbeat sensor is embedded avoiding scan for every action. It seems that the project remains at the research level and there have been no commercial offers since 2014.

• Bionym, a Canadian start-up has developed the Nymi wristband based on a proprietary technology called HeartID using the wearer's heartbeat in place of passwords. The wearable has been designed for physical access control and also for logical access control and it can be used for fitness tracking. Some banks are currently testing the device like TD band and Royal Bank which is commercialised at the price of 199 USD.

Nymi wristband

3

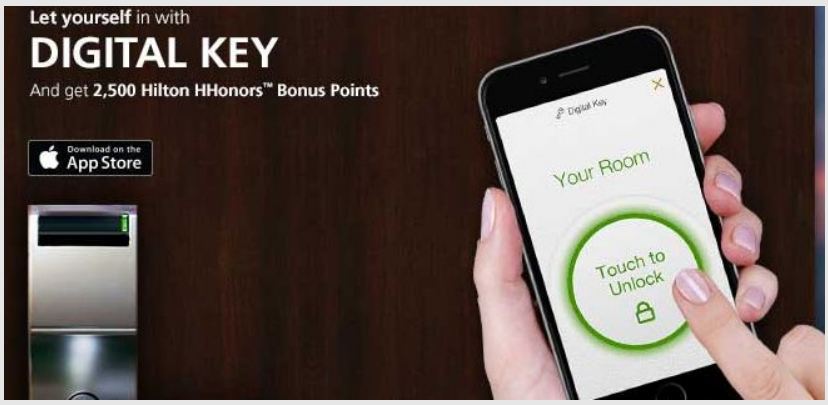
Advanced secure access control solution gaining traction

The hospitality industry is the segment which is the most advanced in secure access control, e.g. allowing visitors access to their hotel rooms using smartphone or wearables. Other sectors are also interested the evolution of secure access control with different types of requirements like using the combination of biometrics along with devices.

The connected hotel

The hospitality industry is considered as one of the leading sectors. Indeed, hotels and event venues are considered as one of the fastest-growing segments of the access control market. In order to remain competitive, those industries can leverage on technology to provide the most customised experience to their customers. Indeed, the concept of "connected hotel" is developing. Guest experience can be enhanced and thus satisfaction improved, too. The idea is to provide customised services during the whole stay (from detection of guests at arrival) by providing up to date information.

Digital key app for Hilton Honors



The use of wearables could be part of the connected hotel concept allowing the guest to use it for different things: room access, check-in, payments, real time information, temperature control in their hotel room, etc.

Hilton has developed its own mobile application called Digital Key, launched in 2015. Dedicated to Hilton Honors guests, the app provides customised experience to frequent guests with the option to bypass the hotel check-in counter and access their rooms, via the Hilton Honors app on their smartphones. In March 2017, Hilton Honors has introduced its Digital Key in 1000 of its hotels, counting 6.4 million room doors that can be opened using the app. Hilton plans to reach over 2500 hotels by the end of 2017.

Healthcare

Security access is primordial in the healthcare sector to protect the assets, the research and trials, to prevent bio-terrorism, but also to protect healthcare personnel (doctors, nurses). Sensitive areas in clinical facilities and hospitals (maternity zones, emergency departments and intensive care units) are also subject to high control due to the large amount of people circulating. The introduction of advanced systems could help staff to move freely and quickly.

Indeed, in hospitas, staff members may need to use a particular entryway up to 100 times in a shift. A free hand (no touch access) solution to open doors could be appropriate in this sector where healthcare staff often have their hands full or for elderly care facilities ensuring the access to the room for only authorised people.

The company Kaba Access has developed a solution based on capacitive identification. The user just needs to carry a transponder (in the pocket, jacket, around the neck, on the wrist or in the bag) and can open the door just by touching the door handle.

The solution has been implemented in nursing homes and retirement homes for dementia patients in Switzerland, Netherlands, Sweden and France.

Industrial sites, defence, military

Sensitive sites, nuclear power plants, defence and military areas are naturally subject to strong secure authentication.

In the US, smart cards are used in many government agencies to authorise access to building as well as network, but have revealed vulnerabilities. In order to counterfeit the vulnerability of card-based systems and for a better efficiency, the Pentagon has issued a Common Access Card for the different

The hand used as a key to unlock the door by Kaba Access

buildings in a single one in 2015; the new system is a combination of contactless cards and biometrics solution (iris and fingerprints) including personal identity verification.

Tertiary sector

Large business offices often located in towers or large sites are also seeking to restrict and control the access to their facilities to employees or visitors. More specifically, banks are focused on secure access control and expect a high level of security. According to an academic study led in 2012[8], some banks were already using biometrics to authenticate employees and customers, of which 52% were located in Asia.

Education

The education sector is also a great market for access control to secure school buildings and protect students from unauthorised individuals. The use of mobile credentials in this sector could be appropriate with a high proportion of the population (college and high school students) already equipped with smartphones.

4

Positive signs for the development of the market

Market drivers

Adoption of smartphones and wireless technologies

The strong adoption of smartphone and other mobile devices as authentication systems could be a key driver for a significant change for the market.

Today, consumers have clearly adopted wireless technologies and especially smartphones for different usages in private and professional environments and are totally part of their lives. In terms of access control, new credential form factors such as mobile devices are expected in the future to offer a secure and convenient way to open doors[9]. The smartphone is considered as the more convenient form as people seldom leave their home, car or office without their phone.

Growing security concerns

There is a clear increasing demand for security and safety especially for the entrance to the office. More and more companies want to monitor and manage flows of people and eventually restrict the entrance for specific areas.

There is an increasing trend from residential and corporations to invest in physical access control with the growing risk of corporate theft, malicious damage and terrorism. Indeed, there is a global willingness to manage identity and to deploy security systems in order to ensure security and privacy.

Timing and lifecycle

Most of the existing security systems were installed 15 to 20 years ago. After 2009, upgrading the systems was not the priority so companies only invested the minimum. From 2014, companies have started to release budgets dedicated to upgrading the systems or replacing legacy cards.

The company Napco Security agrees: "there are a lot of systems out there that have just gotten old. Because of the influx of money, a lot of businesses are spending it to upgrade access control systems. It is a big opportunity."[10]

Reduction of credential costs

New credential forms drive costs down. A comparison between the cost of traditional proximity cards and digital credentials has been showcased by the company AMAG at ASIS advanced security conference in 2016 revealing great cost opportunities through digital credentials.

Costs comparison

Costs of a basic proximity card credential at about **$ 12 or $ 13** (including labour whereas) Costs of digital credential almost nothing

Source: Security System News[11]

Barriers

End users' acceptance

According to the manufacturer Assa Abloy, in the access control industry, it takes more time for people to accept to change compared to their personal lives. "Whatever technology will eventually dominate the world, it will take longer in the security industry than it did for smartphones to take over in cell phones."

Also, for solutions relying on biometrics, a key issue to be considered could be the users' acceptance.

Sector slowly changing

The access control market has been historically slow to change so the migration to new systems may take time. Today, the market is stuck with card-based systems, often proprietary where smart cards and also biometrics have been long awaited but not reaching mass market. Indeed, some access control solution suppliers like Tyco see their customers as conservative. The life cycle of the card is estimated at 10 years (and even 20 years) so as far as the system works there is no need to change.

References

[1] http://www.sdmmag.com/articles/93709-state-of-the-market-access-control-2017

[2] https://www.asdreports.com/market-research-report-280654/access-control-market-global-forecast

[3] http://www.sdmmag.com/articles/92217-state-of-the-market-access-control-2016?page=3

[4] http://futurelab.assaabloy.com/en/the-wireless-access-control-market-in-2016/

[5]ttps://www.asmag.com/rankings/security50_rankings.aspx

[6] https://www.ramarketing.com/quick-fire-marketing-9-amazing-mobile-marketing-statistics/

[7] https://www.ifsecglobal.com/the-physical-access-control-market-same-customer-value-equation-new-dynamics/

[8]http://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202(9)9152-9160,%202012.pdf

[9] http://cloudastructure.com/blog/mobile-physical-access-control-a-new-approach-for-opening-doors/

[10] http://www.sdmmag.com/articles/91029-state-of-the-market-access-control

[11]http://www.securitysystemsnews.com/article/market-trends-mobile-access-control-today-where-are-we

About the Digital Transformation Monitor

The Digital Transformation Monitor aims to foster the knowledge base on the state of play and evolution of digital transformation in Europe. The site provides a monitoring mechanism to examine key trends in digital transformation. It offers a unique insight into statistics and initiatives to support digital transformation, as well as reports on key industrial and technological opportunities, challenges and policy initiatives related to digital transformation.

Web page: https://ec.europa.eu/growth/tools-databases/dem/

This report was prepared for the European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs; Directorate F: Innovation and Advanced Manufacturing; Unit F/3 KETs, Digital Manufacturing and Interoperability by the consortium composed of PwC, CARSA, IDATE and ESN, under the contract Digital Entrepreneurship Monitor (EASME/COSME/2014/004)

Authors: Vincent Bonneau & Tiana Ramahandry, IDATE and Laurent Probst, Bertrand Pedersen & Lauriane Dakkak-Arnoux PwC