NB IoT Smart Access Control Business Case

Version 3.0 March 2020

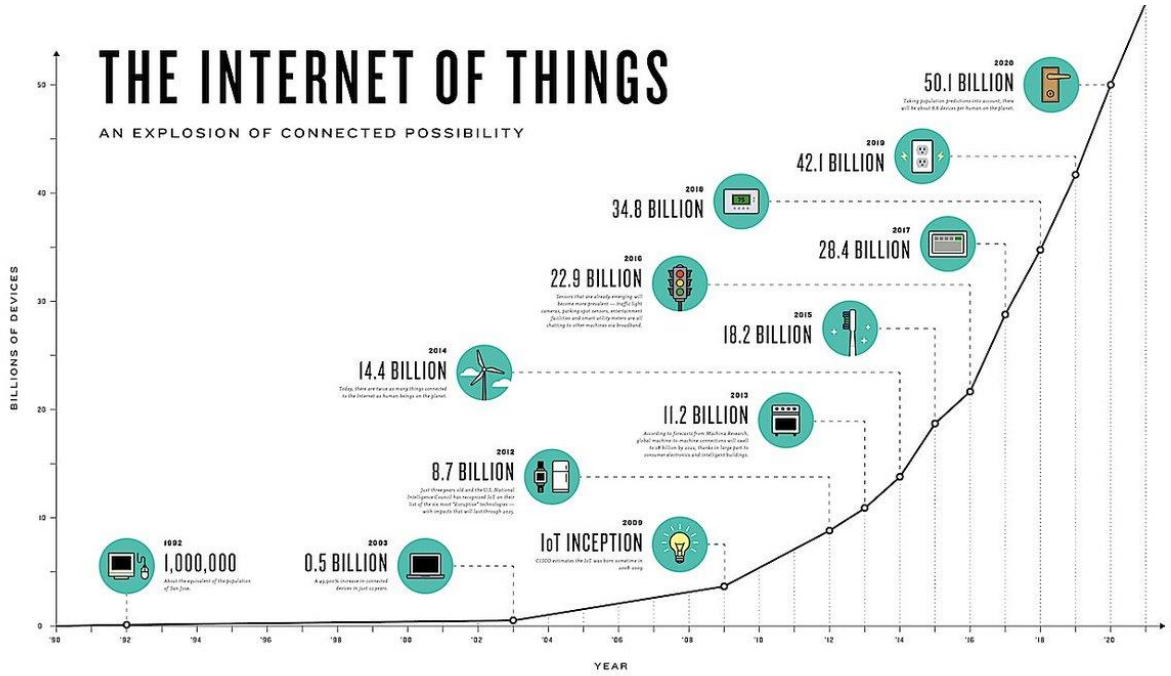
Foreword

The **'Internet Of Things' (IoT)** is about the extension of internet connectivity into physical devices and everyday objects. The IoT market is expected to be bigger than the smartphone, tablet, and PC markets combined, expecting to double by 2021 to $520B[1] with connected locks sitting at the top of projected IoT device sales over the next five years (see graph below).

'NarrowBand-Internet of Things (NB-IoT)' is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services to communicate and connect to the Internet. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Battery life of more than 10 years can be supported for a wide range of use cases.

Supported by all **major mobile equipment, chipset and module manufacturers**, NB-IoT can co-exist with 2G, 3G, 4G and 5G mobile networks. It also benefits from all the security and privacy features of mobile networks, such as support for user identity confidentiality, entity authentication, confidentiality, data integrity, and mobile equipment identification. The first NB-IoT commercial launches were completed in 2016 and a global roll out has been underway over the last few years with over 50 Telecommunication companies now adopting NB IoT on their mobile networks, with full nationwide coverage in around 40 countries, with NB IoT launches/partial nationwide coverage in 74 other countries[2].

This report provides an analysis of **'NB IoT based security systems**', which are about devices, such as locks and alarms, embedded with electronics, Internet connectivity, and other forms of hardware (such as motion sensors) which can communicate and interact with others over the Internet and NB IoT network via API's, and they can be remotely monitored and controlled by people with software and apps or artificially intelligent systems.



[1] ***NCTA -The Internet & Television Association, Washington DC, USA***

[2] https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

Executive Summary

Globally, the **access control industry**, sometimes referred to as the '**physical security industry'**, is in the midst of a transformative process of integrating wireless technologies and **IoT** into the traditional keycard access control system to deliver more efficient and responsive services to customers.

When adding wireless internet connected technologies such as Wi-Fi/BLE and their related processes to access control, the terms "smart locks" or "smart access" or "smart access control" are used. Smart access has different definitions and implications depending on one's perspective.

- **From a regulatory perspective**, smart access fosters meeting government compliances, e.g. PCI – restricting access to rooms that have PC's that process credit cards; and tracking employees for meeting OH&S regulations.
- **From a Property/Facilities Managers perspective,** smart access is about delivering security, controlling access to assets/buildings, and more efficient key management leading to cost and time savings.
- **From a customer perspective**, smart access offers more convenient access, safety and peace of mind.

Regardless of the perspective, enterprises must address workplace regulations, and customer/staff expectations by adopting smart access control.

However, the speed of smart access adoption has been very slow. For example, in a 2018 poll set out to gauge perceptions of, and demand for wireless technologies, carried out by the world's number one lock manufacturer Assa Abloy, to hundreds of professionals involved in the procurement, operation, deployment or maintenance of access control systems in enterprises, revealed only 6% of installed electronic access systems in enterprises are fully wireless[3].

The slow adoption rates of smart access can be attributed to higher costs of wireless products, unreliability of wireless technologies, and the need for significant onsite network infrastructure (such as Wi-Fi mesh networks). But the main reason for slow adoption is often attributed to hacking and 'fears of hacking'. All existing smart access control technologies including, Wi-Fi, Bluetooth, Zigbee, and Z-Wave and others have recently been exposed as hackable.

In addition to making a product work perfectly all the time to avoid lockouts, the physical security industry has obviously always been concerned with security. But in more recent times, physical security companies/lock manufacturers have to think about data breaches because of the nature of the data being communicated, and they must follow protocols to harden their products and make them less susceptible to compromise, attacks, and tampering. Enterprises customers in particular are demanding cyber security processes and protocols, as they don't want to risk putting anything on their network/in the cloud if adequate safeguards are not in place.

The global resistance to smart access control adoption can be evidenced when you compare the number of smart electricity meters already installed around the world, with over 64 million installed in 2015 alone in the USA[4] compared to only around 1 million smart locks installed globally in the last 5 years[5]. There is significant global apprehension around IoT-enabled physical security, and the only way to overcome this fear is to offer a new more advanced technology for smart access.

While cyber-attacks are not new and have been around for as long as the internet has existed, the unprecedented level of digital transformation occurring across all industries has resulted in cyber-attacks becoming much more frequent and costly these days. The growing amount of valuable data

[3] [3] https://www.ifsecglobal.com/global/exclusive-download-the-wireless-access-control-report-2018/

[4] https://www.eia.gov/tools/faqs/faq.php?id=108&t=3

[5] https://nextmarket.co/products/smartlock

being digitised is prompting cyber criminals to employ increasingly sophisticated ransomware and malware, resulting in attacks that have far reaching consequences.

The physical security industry, which has not changed much in the last 2000 years (since ancient Romans invented the metal key and lock), is prime for disruption so it can meet the needs of enterprises in these 'cyber insecure' times.

What the physical security industry needs now is a new IoT communications technology for use in smart access control with unprecedented levels of security, but at the same time is reliable, convenient, does not have any onsite infrastructure and which enables long battery life for devices.

A new IoT communications technology called **Narrowband IoT(NB IoT)** has been developed by telecommunication companies that utilizes all the inbuilt security features and encryptions of mobile networks, to meets all the physical security industry challenges it currently faces.

Read on to learn more about NB IoT and current trends in IoT and the physical security industry. You'll also discover how your organization can become more secure with NB IoT smart access…

PART 1

The business case for companies and business to adopt NB IoT Smart Access Control Systems

What is smart access control?

Access control is defined simply as 'the selective restriction of **access** to a place or other resource'.

Smart access control is generally defined as a combination of 'traditional access control' (i.e. with keycards/software or metal keys), with '**smart controls via the internet**' (i.e. with cloud-based software, smartphone digital keys, data analytics etc.).

Whilst '**smartcard'** access control has been around for about 30 years, it should not be confused with **smart access control.** Smartcard access control systems are generally disconnected from the internet, where-as **smart access control systems** connect to the internet and so provide other features such as smartphone digital key unlocking, live audits, and big data analytics.

Smart access control also has different definitions and implications depending on one's perspective.

- **From a regulatory perspective**, smart access fosters meeting state and federal Occupational Health and Safety (OHS) requirements, Critical Infrastructure Act requirements, specific industry requirements (e.g PCI credit card compliance), and meeting requirements regarding employee wage theft. Smart access helps meet these requirements/regulations by being able to;
  - track employees' arrivals and movements around a work site and multiple work sites with digital keys and live audit notifications to manager's phones.
  -know who is on site at anytime, and recording that data, to meet company reporting requirements for insurance implications
  -controlling access to specific rooms to meet compliances for protection of machines/devices that store or process data for PCI compliance for credit card processing, and for the safe storage of personal/private data of employees and customers such as in storage cabinets.
- **From a Property/Facilities Managers perspective**, smart access provides enhanced security, access control, data management and analytics, and more efficient key management leading to cost and time savings.
- **From a customer perspective**, smart access will offer more convenient access, better safety and peace of mind.

Regardless of the perspective, any company that operates out of at least one physical building, must address regulatory expectations, in addition to addressing staff and customer expectations regarding safety, access, security and data management.

Smart Access Control to meet industry standard Government mandatory regulations.

Certain industries must meet their own specific set of mandatory regulations, and smart access control can be used to help meet those regulations. The security principles in regulations usually refers to protection of system resources against unauthorized access. Smart Access Control helps prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information

For example, **hospitals, doctors' offices, and health insurance companies need to comply with HIPAA health data regulations** regarding controlling and restricting physical access to rooms/cabinets that hold patient's folders/data and medicines.

Smart access control can also support enterprises in the **financial services industry** meet mandatory government regulations regarding credit card processing. Banks, insurance companies, and any business that accepts and processes credit cards are subject to PCI credit card data regulations regarding restricting access to the public and most staff to computers/servers that house customer's personal information. Smart access can provide access to certain individuals to certain rooms for limited time periods which they can unlock with their smartphones, and at the same time an audit is stored for each room's unlocking activity.

Finally, any business that deals with privileged data and intellectual property, needs to meet **Security Operating Center (SOC) cybersecurity regulations**. Examples of businesses needing to meet these regulations include Software as a Sevice(SaaS) providers; data centers, software developers, entrepreneurs, startups, and pharmaceutical companies.

Smart Access to meet employee duty of care.

Regarding **staff safety, employers have a responsibility to ensure the health and safety of their employees in the workplace**, and they must set the protocols and make sure the workplace is compliant with regulatory standards. This is often referred to as the **'employer duty of care'** responsibility. As part of this duty, your boss, by law, has the right to know where you are, and the work environment must be secure and safe. For example in most office environments the general public should not be able to roam around hallways and into private offices.

Employee location tracking as a feature of smart access can provide improved worker security and safety, especially when managing evacuation procedures during an emergency.

In addition, tracking worker locations can enable many other workplace applications with a wide range of benefits including improved productivity; increased safety; and reduced costs. For example, productivity can be improved when it becomes easier and quicker to move around different sites and locations; increased safety can occur by restricting public and staff access to specific buildings/rooms/sites; and reduced costs can occur from not making staff drive across town to pick up metal keys to access multiple sites (and then driving back across town to return them again at the end of the day).

In the past various efforts to track employee movements with GPS and mobile phones/apps have faced employee backlash due to privacy concerns, and it has exposed companies to legal actions due to grey areas in local laws. Smart Access control can avoid privacy concerns of apps and GPS trackers, particularly worrying as the apps keep on tracking 'after hours'. Smart access systems avoid privacy concerns by acting like a traditional 'punch card log-in system', recording in a cloud database who opened which door at what time (and also providing live text/email notifications to managers mobile phones).

The analysts view

Don't forget people are also motivated to get smart access control, because of the nuisance in having to carry around metal keys everywhere you go!

Other motivations for adopting Smart Access

Smart access also provides increased information flow, where the users can make quicker, more informed decisions about the system's use and how to optimize it. This information flow occurs through the increased use of lock audits, and the locks communications and interfacing capabilities (for example through API's linking the locks to third party software and hardware) arranged to gather, transmit, decode, and analyze and share raw data into useful information and actions. These features will become increasingly automated with AI as technologies such as NB IoT and 5G advances. For example, Real Estate Agents can set up software and apps that enable registered 'house hunters' or 'potential tenants' to download time-sensitive/one-off digital keys to 'self-inspect' vacant

houses for sale/rent, without the need for Real Estate Agents to go out to the houses and unlock the properties to let people in for open inspections. The digital keys can also be interfaced to the alarm system, so the alarm automatically turns off when the authorized digital key is entered on the front door, and the alarm can automatically switch on again in say 30 minutes, giving the house inspectors time to roam throughout the house, and leave.

Devices, access control systems, IoT applications and other solutions connected to the Cloud will provide robust data for advanced analytics. Insights from these analytics can be used to optimize workflow solutions and provide more seamless access for end users. For example, for employees that need to access multiple sites on a regular basis, such as social workers/nurses visiting clients homes, or workers of utility companies, or postmen/courier contractors, they can get the most efficient schedules and access credentials to different sites mapped out/emailed for them **automatically** each day in advance (and which can update at any moment) rather than individuals wasting time planning routes, schedules and chasing down and returning metal keys.

Predictive analytics will play a crucial role in people-centric security and access control, and address employee demands for workplaces to deliver premium, more individualized services. Analytics will also help reduce downtime in the enterprise, spur factory automation and improve compliance via condition monitoring that is based on real-time location and sensing solutions.

Smart Access Control Comparisons

Smart Access control solutions can be built on a variety of technologies which connect to the internet or to other devices/software. Currently the most common technology used for smart access control is Wi-Fi/Bluetooth Low Energy (BLE) technology.

A comparison of smart access control systems including Wi-Fi/BLE vs NB IoT vs RFID keycard systems is offered in the tables below.

	RFID Keycard Systems
Time-sensitive access control	✓
Set up costs	Approx USD$6000
Costs per lock	USD$500-$5000
Onsite Infrastructure	Wiring, card encoder box, onsite PC/software, controller box, programmer device
Battery Life	Mains powered
Online Solution*	✗
Security	Hacked; subject to man-in the middle attacks
Multiple locks use	✓

	Wi-Fi/Bluetooth systems	NB IoT Systems
Time-sensitive access control	✓	✓
Set up costs	Approx USD$300 Wi-Fi systems (routers, modems, bridges)	USD$0
Costs per lock	USD$300-$500	USD$300-$500
Onsite Infrastructure	Router, modem, ISP, cables, bridge, boosters, phone line	nothing
Battery Life	6 -12 months	1 and 1/2 years
Online Solution*	✓	✓
Security	128 bit SSL encryption + congested, unstable, inscure network. Hacked	2048 bit RSA encryption + 128 bit SSL encryption + DLTS + VPN + licenced network
Multiple locks use	✗	✓

Smart Access Adoption Impediments

Impediments for companies and organizations to move ahead with transformation to a smarter access control system include;

- Fears of cyber security
- Fears of new technologies
- Skepticism regarding benefits as compared to costs
- Resistance to change

To further complicate the situation, motivations to adopt smart access is different for each enterprise and industry. After all, each enterprise and their staff/customers have unique access requirements, unique legacy access control systems, and unique safety concerns shaped by individual's activities, company building design, multiple company sites, and workers past experiences with metal keys or keycards. These unique motivations will be explored in detail throughout this next section.

How NB IoT addresses fears of cyber security/new technologies

Unlike some forms of internet connectivity, NB IoT networks are carefully managed and secured by mobile operators/telecommunication companies with standardized security to guarantee the credential and integrity of all data running through it. NB IoT has passed security protocols as outlined by 3GPP, and the GSMA, the organisations responsible for managing the mobile networks. These organisations have also officially licenced NB IoT for global use in machine to machine to internet/cloud communications, and it is the only licenced technology for this. All other machine to machine/IoT communication technologies such as Lo-Ra, Sigfox and others are new, unlicensed, unregulated, uncontrolled and insecure. Some of the security features and safeguards built into the NB IoT networks by the mobile operators, who have spent over 30 years and billions of dollars perfecting for use in their mobile networks, include;

- All communications are running on HTTPs military grade 256-bit encryption including on all vertical layers between software and hardware, plus 2048 bit NB IoT chipset encryption
- Between the telco's mobile network, and the IoT device management platform a layer of Internet Protocol Security (IPSEC) is provided.
- A dedicated VPN is provided for device manufacturers for further security and reliability.
- the device that sends data to the cloud is authorized and so it cannot be replaced/altered with by another.
- a communications observer cannot understand the encrypted messages and only the cloud with the decryption keys can retrieve the messages, so there can be no hijacking of devices by botnets and others.

By supporting an array of security features and safeguards such as those mentioned above, NB IoT networks are set to play a pivotal role in building trust in the Internet of Things, while giving enterprises the confidence they need to bring mission-critical assets online, so they can be remotely monitored and controlled. Included below is a more detailed list of security and safeguard features for NB IoT offered by OpCo's.

3GPP & ETSI Global Security Standards	
IP Network	Optional
Algorithm Negotiation	
Critical Infrastructure Class	Access Classes 11-16
Reliable Delivery	
Identity Protection	TMSI
Updatability (Device)	Possible
Updatability (Keys/Algorithms)	Optional (SIM OTA)
Network Authentication	LTE AKA
Data Confidentiality	
Data Integrity	Optional (with DoNAS)
Network Monitoring and Filtering	
Device/ Subscriber Authentication	UICC or eUICC
Control Integrity	
Globally Unique Identifiers	IMSI
NB-IoT chipset Encryption	2048 Bit RSA encryption
Military Grade Application Security	

The existing technologies used in smart access control such as Wi-Fi/BLE have been designed for human connections and not machine connections, so they are antiquated, fragmented and non-standardized. Shortcomings include;

- poor reliability
- poor security
- high operational and maintenance costs
- high set-up and infrastructure costs.
- Low battery life
- Poor connectivity/integrations across platforms and devices

In October 2017, a massive security vulnerability called KRACK, effected Wi-Fi devices and smart locks. The KRACK hack allowed hackers to hijack your W-Fi connection, inject content, steal passwords, and monitor your traffic. The security and access control industry, recently plagued by hacking scandals, is seeking out a new technology to rely on - NB IoT can be the answer. A summary table is included below of some of the recent hacks for access control technologies.

Technology	Hacking/Insecurity
Bluetooth	In mid 2016, over 75% of Bluetooth smart locks on the market were shown to be open to hacks. Many research papers were published online, showing vulnerabilities in Bluetooth locks, and how a device costing around $100 can unlock any Bluetooth lock. Besides being insecure, Bluetooth smart locks are also difficult to pair and are unreliable. https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/
RFID	In June 2017, RFID keycard locks, commonly used in offices and hotels, were shown to be easily copied at a DEFCON conference using a cheap device costing $10-$20. With this device and some code available online, hackers can easily remotely copy your keycard credentials, and let themselves into your office/hotel room in under 30 seconds. Also the same technology is used in car key fobs, and in mid 2017, a spate of car break-ins using the RFID hack have been happening all over USA and Europe. https://www.redteamsecure.com/tech-insider-how-to-covertly-steal-and-clone-rfid-badges/
Magnetic Stripe	Back in 2012, over 4 million magnetic stripe locks in hotel rooms were shown to be hackable and easily opened with a device that cost less than $20. More recently, more and more hacks exposing magnetic stripe technology, also commonly found in credit cards as well as hotel rooms, became evident including the Target credit card hack which exposed 40 million people's credit card numbers in the US in 2014. https://null-byte.wonderhowto.com/how-to/turn-innocent-dry-erase-marker-into-hotel-hacking-machine-0139534/
ZigBee	In 2015 Researchers at Black Hat and Def Con warned about security flaws in Internet of Things devices using the ZigBee protocol, leaving Philips Hue light bulbs, zigbee smart locks, motion sensors, switches, HVAC systems and other smart home devices vulnerable to compromise. https://www.csoonline.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html
Z-WAVE	In 2016, a Z-Wave hacking tool was demonstrated at a hacker conference and was shown to be physically capable of destroying Z-Wave devices. https://suretydiy.com/can-hackers-unlock-my-z-wave-door-lock/

How NB IoT addresses skepticism regarding benefits as compared to costs, and resistance to change

The enterprise embracing smart access control will realize that new smart building products will continue to be developed in the future, and these products can easily be interfaced onto the one NB IoT platform for further integration as smart building systems mature and confidently 'grow together' without the risks of hacking.

Having a mixture of technologies in building management devices, is not only insecure, but it can also be difficult to achieve, as all these technologies don't always play well together. For example if you have Wi-Fi/BLE smart locks, it can be hard or impossible to get them integrating with Z-Wave burglar alarms, whilst also integrating with wired smoke alarms and CCTV.

NB IoT smart devices can be integrated into legacy devices and systems, and bring other older 'disconnected' systems online so as to take advantage of all the requirements and benefits already discussed.

For example, if you have an existing RFID keycard system in your building, you can install NB IoT smart locks, which also contain NFC technology, and transfer digital key/unique key ID's onto NFC stickers which can then be stuck on existing RFID keycards. You don't necessarily have to rip out legacy systems. Taking this one step further, the underground car park gate, can be connected with NB IOT and the gate digital key can

be added to the NFC sticker too and stuck onto the RFID keycard.

Further, as mentioned in the previous section, NB IoT smart access also represents a unique opportunity for enterprises to get a taste of big data analytics, automations, and predictive AI. Enterprises can start with NB IoT access control and build an appetite to further adoption of other smart buildings products/services NB IoT smart electricity metering, NB IoT smart parking, and NB IoT smart lighting.

The improved data management that comes with smart access provides more detailed information about the status and operation of all buildings and for the entire enterprise for use in its decision making, planning, and operations. This use can lead to significant costs savings/increased profits from improved hour-to hour management, improved short- and long-term investments, better resource planning, improved forecasting/financial planning, and improved customer service.

Enterprises adopting NB IoT smart access can also be introduced and educated about the value that NB IoT connected devices bring to their enterprise, so they will constantly demand other smart products and services built on NB IoT technology in the future.

Demands of NB IoT Smart Access from enterprises

The sections below discuss some relevant functionalities of NB IoT smart access control that can be offered to the large enterprise customer. Unlike their Wi-Fi/BLE access control counterparts, most of the features below can only be offered with the use of NB IoT.

To meet their security requirements for wireless access control, enterprises demand a system architecture/management system that is cloud-based, SaaSstyle, with the underlying infrastructure operated, managed and maintained by a trusted company such as a telecommunications company, or companies with strong cloud services such as Amazon.

In addition, the cloud vendor shall guarantee near 100% availability of any cloud component of their solution. The system architecture should also be fully documented and include all system components, ports, protocols, interfaces, etc.

Management and hosting of the platform should be through a single administration portal, that does not rely on multiple consoles, so there is no need for onsite infrastructure, and the system can be managed from anywhere. The management system must be able to use Active Directory-based authentication for administrative users and for role-based access. Visitors must be managed locally by the system. The apps must synchronize with Active Directory on a regular basis to ensure access is removed from the application in a timely manner once a user's account has been disabled.

The management system must be able to alert an operator/account administrator if an access control device is unavailable, has low battery, or is being tampered with. The management system must be able to show a map of all the enterprises buildings/assets and the location, health and status of access control devices should be interactive on the map. The Management system must have a public portal (website log-in/mobile app) for external users to register for new accounts and for access to select buildings/rooms/assets. The system must be able to store a list of rooms/assets for the users to select from. The system must have a mobile app that external users can download easily from the online stores (and receive One Time Passcodes to verify their identity). The issue of credentials to a user's mobile device must be within ten to thirty seconds.

The Management system must also be able to audit the usage of the system and allow administrators to get reports of any user. The system must be intuitive and provide an easy-to-use user experience and be flexible to work outside of normal business hours**.** The solution shall not introduce any additional overhead and latency onto the enterprises systems; user productivity must not be affected. The system must offer automatic update policies, controls and new mobile app versions without connecting directly to the enterprise's network.

Lock functionality demands

The locks must be able to synchronize access control lists (user names, upcoming digital keys generated, expired digital keys etc.) on a near real-time basis regardless of location or connection type. The locks must support a variety of opening methods including card based (such as with NFC) and staff and visitors must be able to use their mobile device as their credentials; metal key overrides should be available. The locks must be compatible with standard doors and should not require custom door hardware to work. The locks must have both visual and audible feedback for users to identify if their access is authorized. The locks should be of a variety of designs, from lever locks, to mortise locks, to deadbolts, to deadbolt attachments, to knobset locks, and padlocks.

Integrations

The system must allow for secure API based integrations with other systems, such as CCTV systems, intrusion alarms, door open to long alarms, etc., to allow for the enterprise to further extend the use of the smart solution. These API's should use standard, open protocols that allow for interoperation with other systems and devices and supports the use of an application proxy that brokers the connection between the cloud. The API's should not store data temporarily on disk to facilitate the transfer of data between applications.

The system should allow the enterprise to produce reports for PCI compliance, such as being able to download/export audit logs as CSV files for use in spreadsheets and databases, and data analytics.

Specific security feature demands

The system should enforce the encryption of all data in transit using a minimum of 128-bit key length. The system forces the use of TLS 1.2 only, and SSL v3.0 and TLS 1.0 are disabled by default in addition to Security Assertion Markup language (SAML) authentication. The system should be tested against the OWASP Top Ten (the Most Critical Web Application Security Risks). The system has been subjected to vulnerability or penetration testing. The system has SSL certificates/wildcard certificates and supports enterprises existing certificates. The system uses secure infrastructure to download automatic updates and updates are validated before they are installed. The system does not use open source components and supports IP whitelisting. The system encrypts data at rest or encryption is implemented at a higher level, for example Transparent Database Encryption (TDE) is enabled, and a description of what data is encrypted should be provided. Monitoring for data tampering and integrity takes place and the application alerts the user if any suspicious transactions are found.

Static and dynamic code analysis should be performed at regular intervals to test for security vulnerabilities. Cryptographic keys should be stored securely and managed throughout their lifecycle. Access to the keys should be restricted, audited and logs retained. The system should incorporate multi-factor authentication in to the user login and is capable of allowing enterprises to configure things such as; passwords length, passwords being salted/hashed, password history, expiry, blacklist, complexity (i.e. with numbers, letters, special characters etc.), session log out times, number of log-in attempts before lockout etc.

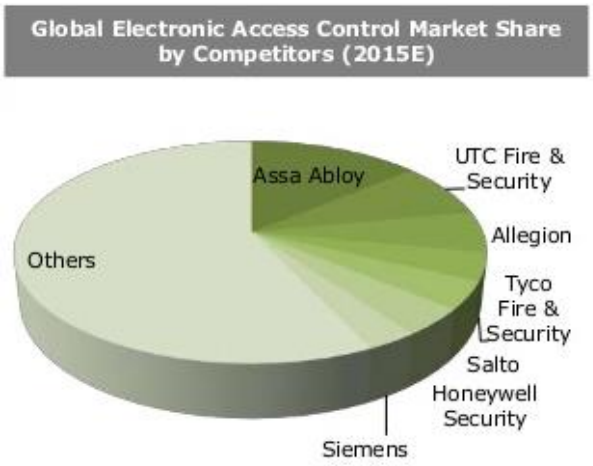
The data center's where the application is hosted is preferably local (within national boundaries) and certified to meet certain Government regulations.

Future Integrated System Development

A long-term consideration of many enterprises that are evaluating improvements to building/facilities infrastructure, under the smart building umbrella is 'the advancement of a fully integrated system'. This advanced fully integrated system will effectively connect, monitor and coordinate company resources whilst reducing expenses via intelligent control logic and communication networks. Upon prioritizing the desired smart access control functionalities discussed above, a more comprehensive smart building implementation strategy and plan can be derived by the OpCo and offered to the enterprise customer.

Access Control Trends and the implications for NB IoT Smart Access

This next section includes an analysis of an 'Access Control Trends Report'[6]' carried out in 2019 by HID Global - an American manufacturer of secure identity products. The company is an independent brand of Assa Abloy, a Swedish door and access control conglomerate – and the number one physical security company in the world – see graph below.



The trends in the HID global report provide a good snapshot of the overall access control and physical security industry globally and highlight some issues to watch now and into the future.

At the time of the HID report, the use of NB IoT in access control did not yet exist in the marketplace, and so it was not featured in any of the HID surveys/report findings. For the purposes of this Business Case, a separate analysis of the HID report findings and its impact on NB IoT smart access, is carried out in each section.

Executive Summary of HID Global Report

Currently there are diverse access control implementations occurring across a variety of industries. Some enterprises are taking an all-inclusive digital/smart approach to implanting access control, while others are selectively incorporating elements for the management of buildings one product at a time.

According to surveys carried out by HID Global as part of the Trends Report, adoption of smart access control in the near future will escalate, as a result of increased awareness of the cloud's ease of deployment, flexibility, connectivity options and productivity benefits. Access control cloud platforms with APIs and SDKs will fuel new software solutions that expand choices for organizations to get the most out of their investments.

Cloud authentication and credential management will further integrate mobile devices, tokens, cards and machine-to-machine endpoints. And digital certificates in the IoT will draw upon the trusted Cloud services to deliver and manage certificates across thousands of devices.

More connected devices and environments will drive focus on securing IoT. Digital certificates will become a core component for adding trust in the IoT by issuing unique digital IDs to printers and encoders, mobile phones, tablets, video cameras and building automation systems, plus a broader range of things like connected cars and medical devices.

Apple iOS 11 "read" support of NFC will fuel adoption of IoT-based applications such as brand protection, customer loyalty programs and other use cases that will further drive the need to enhance security in the IoT.

Smart access will reach tipping point for mass market adoption in the upcoming years. In 2018/19, smart access went mainstream and adoption will accelerate even further in 2020 and beyond. Maturity in mobile solutions and integration into other systems, coupled with mobile's ability to enhance user convenience, improve operational efficiency and provide higher security will drive accelerated growth for smart access and mainstream adoption.

[6] https://futurelab.assaabloy.com/en/wireless-access-control-in-2018/

Convergence of physical and digital security will continue – for example the concept of Physical Identity & Access Management (PIAM) will drive convergence of physical and digital security to a single credential, putting identity at the center of all use cases. Government, finance, energy and other regulated markets will emerge as the forerunners using these solutions for secure access to buildings, email, websites and VPN's.

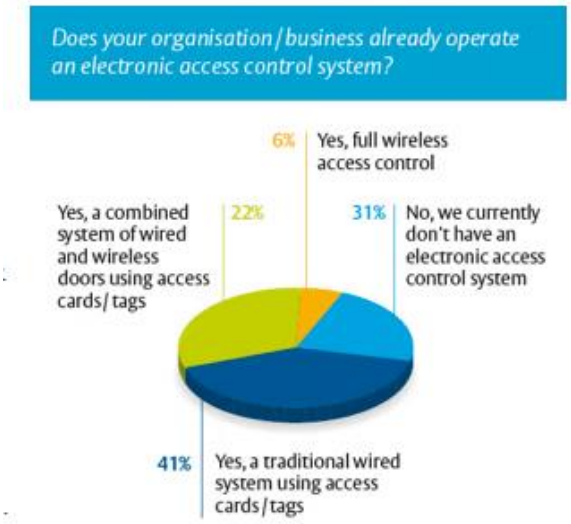
New converged identity models that use cloud authentication and mobile devices are also emerging, such as the ability to verify a person's presence at a location with facial recognition technology, mobile IDs that validate physical citizen IDs, and smart cards that authenticate users to enterprise resources.

HID REPORT FINDING 1: Access Control market is growing at a rapid pace.

Robust growth has been projected in the global wireless access control market between now and 2025, when revenues will reach US$1.66bn at a CAGR of 7.9%. North America, which accounted for 31.3% market share as of 2016, is expected to be the largest revenue contributor. Demand for wireless access control is growing strongly in the residential market, although the commercial arena is still expected to account for 56% of revenues by 2025.

REPORT FINDING 2; Not many commercial businesses have wireless access control systems installed.

HID's poll of hundreds of professionals involved in the procurement, operation, deployment or maintenance of access control systems, was set out to gauge perceptions of, and demand for, wireless technologies in a market where hardwired systems still have an edge. The report revealed only 6% of installed electronic access systems are fully wireless. However, a further 31% include a mixture of wired and wireless systems, and a significantly higher proportion of organizations have wireless systems installed compared to those surveyed at in the previous two years reports.



NB IoT smart access control opportunity based on report findings 1 and 2.

With only 6% of enterprises having adopted wireless access control, the HID report has revealed how wide open the market for wireless access control systems still is. Little penetration has occurred in the marketplace with existing wireless access control systems including mostly Wi-Fi/BLE solutions due mostly to perceptions of insecurity, and costs.

As mentioned in previous sections, NB IoT wireless access control solutions are more secure, more reliable, more convenient, more affordable and require no onsite network infrastructure as compared to their Wi-Fi/BLE counterparts. As NB IoT becomes mainstream and adopted in the marketplace, especially with many other applications such as smart metering and smart parking, we believe the adoption numbers of wireless access control will significantly increase in the near future.

With the wireless access control market still very immature, there is a huge opportunity for NB IoT smart access control to step in as the new 'standard physical security technology' of choice for the twenty twenties and beyond. Its not unusual in the physical security industry to have a technology quickly become standard and be rolled out across the globe. For example in the nineteen sixties, punchcard technology was used in access control, but this was replaced in the nineteen

seventies and eighties with mag-stripe technology. In the nineteen nineties and two thousands, mag-stripe was replaced with RFID keycard technology. In the last decade we've seen wireless connected technologies such as Wi-Fi/BLE attempt to dislodge RFID as the industry standard, but the HID report and industry trends have shown that Wi-Fi/BLE and other wireless technologies such as Z Wave or Zigbee have not had much industry penetration. Other than the hacking and security concerns of existing technologies which we have already discussed in detail throughout this report, most 'wireless technologies' currently available in the marketplace were not designed and built for device to device communications. Wi-Fi and Bluetooth for example were built for humans to connect to the internet for transfers of large amounts of data at a time. NB IoT is built specifically for device to device and device to cloud communications and operations, which generally require very little bandwidth and data transfers. For example an unlock command sent over the NB IoT network typically only uses 5-10 bytes, where as an average sized email sent over Wi-Fi (without any attachments) is around 7500 bytes.

REPORT FINDING 3: Facility Managers/ Security Managers have a more positive view of wireless than five years ago.

With the global wireless access control market growing briskly at a CAGR of 7.9%, such benefits of adopting smart access control are increasingly being recognized by facilities managers and security departments – the key decision makers involved in purchases of physical security systems.

Wireless is "the next natural step in fire safety and security," in the words of one professional who responded to the survey.

Mirroring the usual trajectory of emerging technology, wireless systems have over time become less expensive, more reliable and more versatile. Nearly two thirds (63%) of respondents "have a more positive view of wireless than five years ago because the technology has improved".

NB IoT smart access control opportunity based on changing views of wireless

The decision makers for access control systems in commercial buildings are slowly beginning to accept that access control ***can*** be wireless and secure at the same time. Whilst the decision makers are slowly becoming 'more accepting' of wireless technologies this doesn't mean they are purchasing wireless access control (remember only 6% of survey respondents have wireless access installed on their sites as outlined in previous section). One of the reasons offered by HID surveys for this more recent 'positive view' is that 'the technology has improved'. This is despite news articles and mainstream press continuing to highlight all the hacking concerns with wireless technologies such as Wi-Fi and BLE.

The choices of communications technology currently in the marketplace are still very limited, and all have been exposed as insecure and hackable. As attitudes change towards wireless access control, even with less superior technologies, NB IoT places itself in a good position to swoop in with its more superior and more secure wireless product offering and take advantage of the slowly changing attitudes towards 'wireless access control'.

REPORT FINDING 4 - Existing Wireless access control systems are 20% more expensive than their wired counterparts.

Current wireless locks available in the marketplace are around 20% more expensive than their wired counterparts on average. However, the cost of the additional labor required to make cuts into doors and wire a system can increase the total project cost per door by up to 40%.

NB IoT Smart access control opportunity based on pricing

Existing wireless access control systems, commonly built on Wi-Fi/BLE can be more expensive than their

wired counterparts, as an array of onsite network infrastructure is often required such as modems, routers, gateways, controllers, bridges, mesh access points, servers, and programmers. Further, the installation of most wireless access control systems is complicated requiring a complex mesh network, and a tailored, complex onsite setup.

NB IoT smart access is around 50-80% cheaper than existing Wi-Fi/BLE and other wireless access control systems as there is no onsite network infrastructure whatsoever. NB IoT smart access is also cheaper than all wired technologies too. The reasons for the more affordability of NB IoT smart access is because smart locks are fitted SIM cards, and NB IoT modules (that work like modems) enabling the locks to connect to the local NB IoT networks on the telecommunication companies' mobile networks. Nothing else is required onsite. All the software and systems running in the background, as well as customer facing software is hosted in the cloud and on smartphone apps. And the connectivity costs are very low too - from as low as 10 Euros for 10 years for very low data plans (costs vary depending on data usage/operator).

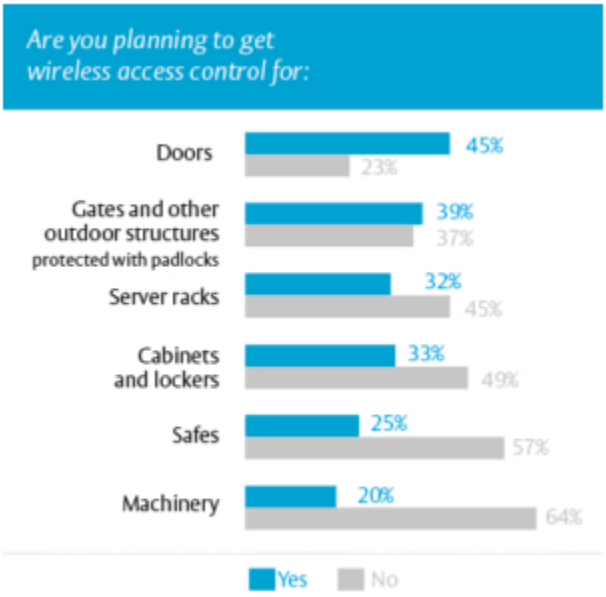
REPORT FINDING 5 - Existing Wireless access control systems demands increasing for 'non-door' applications.

Survey data from the HID report highlights the growth potential of wireless access control solutions for "non-door" applications like parking gates, server racks, lockers, cabinets and lifts. Real-world use cases are not hard to imagine. Cabinet and locker locks are widely deployed in universities, healthcare settings and sports facilities.

Padlocks are popular with critical infrastructure providers including utilities, who often have dispersed, outdoor sites where traditional cabled access control is not a realistic option. The boom in co-location for corporate servers makes server rack locks a popular choice for ensuring data security even when a physical storage facility is off-site.

Partly, the increased demand for 'non-door' smart access is about convenience - the more applications that can be secured and unlocked with a single credential, the better for users. Facility managers benefit from the wider scope of their access system, which gives them more control. In addition, because these 'non-door' devices are wireless, access control can easily extend outdoors. Padlocks for gates, machinery locks, storage lockers: with the right lock, these can all be secured within the same access control system as your front door.

It is anticipated that market growth in this particular sub-sector will out-perform the overall market, with a projected CAGR of 12.9% to 2025.



NB IoT Smart access control opportunity for 'non-door' applications.

As already outlined, most existing wireless access control technologies require onsite network infrastructure such as reliable Wi-Fi networks to be installed, paid for, and maintained, so this restricts the environments for 'non-door' locks/systems. For example an outdoor structure, a gate or a piece of machinery in a yard, will most likely not have a good local Wi-Fi connection available to enable the padlocks to connect to the internet and other devices.

NB IoT requires no onsite network infrastructure, and has penetration 20% beyond the normal mobile networks, enabling greater reach into basements, and on to tops of hills for example. You may typically find critical infrastructure base stations on tops of hills, and the Critical infrastructure companies cannot be expected to install a new reliable Wi-Fi network at every base station just for one or two padlocks on a gate, and then trust that that Wi-Fi connection is reliable and is properly maintained, and works every time.

Also having locks configured to different Internet Service providers on different sites and locations, can often make it difficult or impossible for the locks to communicate with each across multiple sites. NB IoT addresses the 'non-door' application opportunities in the most affordable, reliable, secure and logical way.

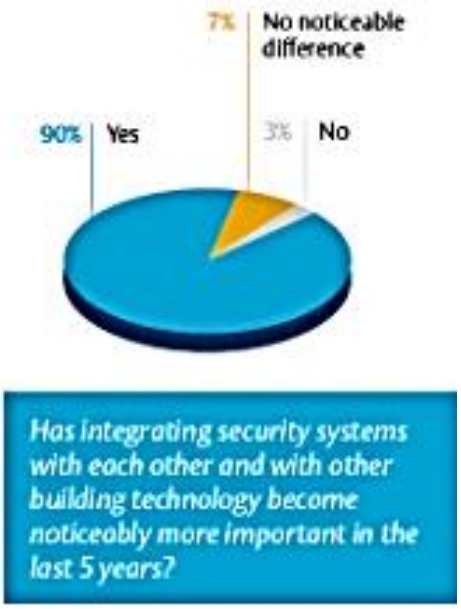
REPORT FINDING 6; Demand for smart access control, integrated and controlled from a single system, is growing.

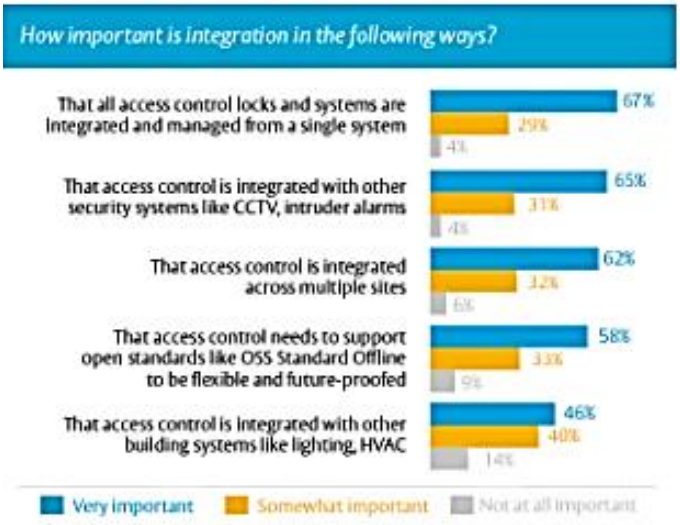
An overwhelming majority of security professionals — both in the survey and anecdotally on the ground — recognize a growing importance of integrating multiple security technologies within a single environment. That is having everything connected to the one platform.

Interoperability is critically important for any end-user investing in new or upgraded access control. They need to plan for eventualities they may not even see yet. Ending reliance on a single, proprietary solution makes installed access control more flexible. You can add a new building, for example, and bring its access control into the existing system seamlessly. Procurement decisions are made with the long term in mind. For buyers and manufacturers, the future is now.

End User insights

"The more applications that can be secured and unlocked with a single credential the better for users".





NB IoT Smart access control opportunity linked to demands for a 'single system'.

NB IoT makes scaling-up with one single system more cost-effective and future-proofs any large investment in access control — and most investments in security, of course, *are* large.

As already outlined, NB IoT adheres to all the latest security standards, meaning all current (and future) requirements for devices that also adhere to these standards seamlessly, communicate within and throughout the entire NB IoT system.

Smart Access Control Case Studies

In this next section we outline some examples of the unique motivations for smart access control for different industries, and take a deeper look into some smart access control project installation case studies.

The benefits and motivations for adopting smart access control vary from industry to industry and company to company - some of these were discussed in section 1 about meeting state and federal regulations, but some other more specific motivation examples to certain industries are discussed below.

Hospitality Industry - improve customer service and for cost savings in not having to staff an onsite reception desk 24/7 or at all. Bring bookings back from Online Travel Agencies to guest loyalty apps with digital keys and self-check-in.

Construction Industry - secure sites early in the construction phrase to safely store and receive building materials through simple distribution of digital keys to builders phones and delivery contractors phones.

Health Industry - to protect sensitive pharmaceuticals/patient information and medicines and improve security for their staff on sites and in car parks.

Education Industry - improve outdated and broken-down mag-stripe keycard systems for controlling access to classrooms, dormitories, and locker locks.

Utility Industry looking to save time and money in not having to make staff drive across town to pick up metal keys to access different sites, transformer boxes, meters etc. and drop the key off afterwards. Tracking employee movements across sites. Receive tampering alerts to notify authorities if people attempt to break open any of their infrastructure.

Office Industry looking to improve their current access control so as to protect server rooms, and improve sharing of meeting rooms. Also looking to provide shared temporary use of office space, like Airbnb does with accommodation.

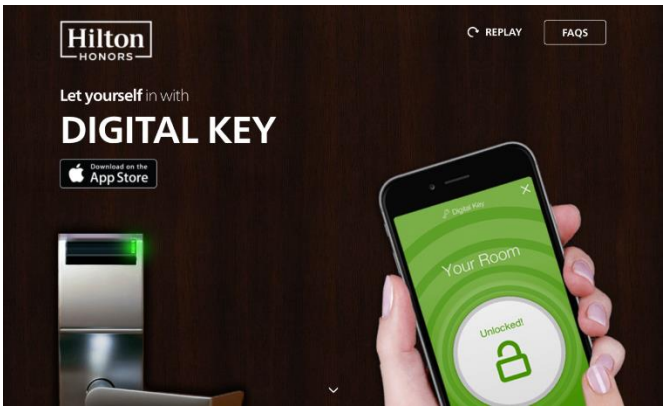
We have included below a brief overview of five smart access control projects in the fields of hotels, sporting facilities, education facilities, and offices, and the reasons for the investment in these projects.

Hilton Hotels Digital Key Global Rollout Project

In mid-2015, Hilton Hotels introduced Digital Key, an all-new feature of the Hilton HHonors app, with the aim of providing the loyalty program's members more choice and control over their entire travel experience.

Digital Key is part of the global technology infrastructure rollout of Hilton's 'Global Digital Strategy', which as seen the company already investing over $550m in this strategy to enable it to bring digital tools to market[7].

Digital Key gives guests the option to bypass the hotel check-in counter and access their rooms with their smartphones, as well as any other areas of the hotel that requires a key, directly via the Hilton HHonors app.



In addition to checking in digitally, selecting their own room from a floor plan or list and using their smartphone as their key, members can further customize their stay via the app by requesting

[7] https://www.phocuswire.com/How-Hilton-sees-digital-today-and-in-the-hotel-of-the-future

amenities – like extra pillows, snacks or drinks – before arrival, or at any other point during their stay.

In 2017, Hilton had rolled out Digital Key in over 362,000 hotel rooms across 2,000 hotels worldwide. In addition, every new hotel that is opened worldwide, roughly one a day, is equipped with Digital Key technology. By the beginning of 2018, Hilton had committed to have well over half of its portfolio of hotels across all 14 brands, equipped with Digital Key, creating a consistent technology experience for guests regardless of where they stay across the globe. Hilton has 5,500 properties with nearly 895,000 rooms, in 109 countries and territories.

The digital key technology includes a refurbishment to their existing RFID keycard locks (adding a small circuit board to the existing lock) to accommodate a Wi-Fi and Bluetooth module. Most Hilton Hotels feature only one or two different types of RFID keycard lock models from just one lock manufacturer, Assa Abloy, which were rolled out in the mid-nineties, making it possible to easily add the small circuit board module in most rooms globally. If Hilton hotels were using a variety of different locks from different brands, then it would be difficult and expensive to make all the different types of circuit board module extensions. The simple refurbishment of one of two lock models, rather than completing replacing the lock on the door offers little disruption to the hotel and guests and has made it possible for a rapid global digital key rollout for Hilton.

Most of the other top 20 global hotel chains have been experimenting with Digital Keys/smart access products for some time, e.g see this Intercontinental Hotel Group article from 2010, discussing their plans to pilot mobile keys https://www.hotelmarketing.com/archive/ihg_pilots_mobile_room_key_solution

However, other than Hilton Hotels, most hotel chains have not yet adopted digital keys/smart access in anything beyond trials, due to the inadequacy, unreliability and high cost of the Wi-Fi/BLE solution currently offered in the marketplace.

The digital key installation has not been all smooth sailing for Hilton and Assa Abloy. Many Hilton hotel guests have also taken to blogs, social media, news outlets and the comments section on the app stores to complain about problems with the digital key such as taking too long to open, opening other locks, and not working[8].

San Mames Sporting Stadium, Spain Smart Access Control Project

In October 2018, the Athletic Club of Bilbao stadium in Spain, otherwise known as San Mamés, installed a smart access control system. Named the best sports building of the year at the 2015 World Architecture Festival, San Mamés can seat up to 53,000 spectators and obviously in a sports stadium of this size and importance, the security system has to perform flawlessly to ensure the site is safe and secure for both staff who work at the stadium and for sports fans visiting on match days.

Smart access control is a vital part of the stadiums security mix, unlike the previous stadium's traditional mechanical key systems. The system installed by SALTO provided a versatile and cost-effective security solution. Facility managers at the San Mamés stadium use it to regulate those who require access to specific areas at specific times, whilst denying admission to unauthorized persons with no right or reason for entry.

The analysts view

The physical security industry is traditionally fixed on hardware, and many lock companies struggle with software.

[8] https://www.executivetraveller.com/hilton-digital-key-review-road-test-using-your-smartphone-as-your-hotel-room-key

Over 200 SALTO Aelement smart locks were installed throughout the stadium, including VIP areas.

This has been developed with the needs of the leisure market in mind and features a range of specific applications including the ability to grant access privileges to individual doors and also gather audit trail data from every door. Other benefits include lost card cancellation, intrusion alarm, door ajar alarm, remote opening, passage mode activation for meeting rooms and automated low battery reporting.

Century 21 (Beggins Enterprises) Offices Florida Smart access project.

Century 21 (Beggins Enterprise) is a top performing real estate group in the southeast region of the United States with over 450 agents in 11 offices spread over the Tampa Florida area. Century 21 reported the following main pain with their security and access control, 'difficultly in granting access to non-agency members' - the nature of the Real Estate industry caters to guest realtors, brokers, lawyers, mortgage agents, and vendors to access the offices on both a short and long-term basis—all of these moving parts can make real estate security difficult to scale. According to Century 21, other pains include 'its annoying to copy 25+ keys or fobs each week for all the different users'.

Since installing the office smart access Wi-Fi/BLE system by Kisi, Century 21 administrators can give certain vendors access, whenever they need it, and restrict the access of other vendors based on the projects they're working on—all from their mobile phone.

The system was set up with a sync to the administrator's Google directory, to onboard employees with mobile phone access credentials.

Hub Australia Co-Working Space Smart Access Project - Sydney

Co-working spaces are becoming an increasingly important sector of the real estate market and one pioneering company, Hub Australia, is on a mission to create a state-of-the-art home for small to large businesses to prosper and grow.

Hub Australia specializes in creating flexible workspaces that provide growing businesses with the resources and learning opportunities to scale their businesses for long term success. Hub strives to provide more than just a place of work, but a community that encourages collaboration, growth and entrepreneurship.

The company operates in three Australian cities, with facilities in Sydney and Adelaide, and more recently, Hub Southern Cross in Melbourne. The new location has tripled Hub's footprint in the city, and occupies 3,900sqm and two floors of the historic Mail Exchange building on the corner of Spencer and Bourke streets. Providing space for up to 700 members, Hub Southern Cross has a variety of areas for one to 20-person teams that includes private offices, open plan dedicated and flexible seating, and for larger company members, bespoke spaces that can be customized to suit.

There are more than 20 differently styled bookable meeting spaces, ranging from a 2 person to 14-person cutting-edge boardroom with the latest technology presentation and conference facilities. Other key features onsite include a, a 50+ seat café, a gym, bike parking, relaxation space, media room, a gallery and an event space for up to 100 people.

Over 90 doors including the main entrance door as well as offices, meeting rooms and locker locks has smart access control installed in 2018.

The Hub Australia facilities manager reported that they liked the cost effectiveness of the solution, and the and the fact that it's scalable and can easily be expanded to meet any future growth needs the Hub may have as and when required.

Cambridge University New Biomedical Campus building smart access project

A new biomedical campus at Cambridge University was recently completed consisting of a three-storey laboratory building and a four-storey office building, housing an innovation centre, laboratories, logistics,

sales, marketing and corporate functions. SALTO Wi-Fi/BLE smart access control is in use at several bio-medical facilities around the world and so they were selected as the smart access control providers for this prestigious new campus at Cambridge University.

Cambridge's new Biomedical Campus Building

Security measures in such places need to be robust and effective with total control over who can access what, when and where at all times.

95% of universities and colleges throughout the world still rely on legacy technology such as magnetic stripes or simple proximity cards for access control - often installed in the nineteen eighties when mag-stripe access control first became popular. Unfortunately, this dated technology leaves these institutions open to security vulnerabilities that often result in increased duplication and fraudulent card use.

As university populations have grown and technology advancements have been made, many institutions are now seeking more secure, economical, and streamlined solutions to meet the needs of their student body and staff - not only for safeguarding people, assets and data - but for connecting students to a myriad of services and applications campus-wide - from physical facility and logical network access to cashless payment and tracking time and attendance.

In order to provide a more secure, convenient and flexible on-campus credential experience to their students, faculty, and staff, forward-thinking universities are now moving away from traditional magnetic stripe (magstripe) and low-frequency proximity card technologies in favor of smart access control.

For Universities smart access control can integrate to their existing student ID card programs (e.g. NFC stickers can be stuck on existing ID cards).

Improved security operations can also create more efficient workflows and easier management of access every semester for students, faculty, and staff. Due to better risk management with the increased security, universities may also experience reduced insurance premiums.

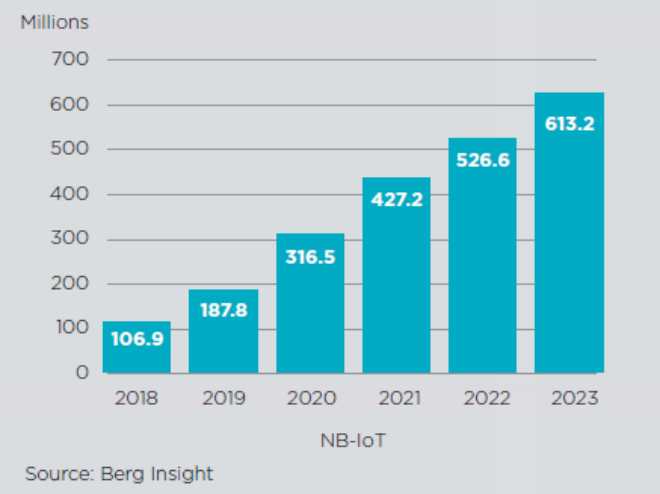
PART 2

The business case for telecommunication companies and their enterprise customers to adopt NB IoT Smart Access

As of mid-2019, 50 telecommunication companies, also referred to as 'OpCo's', have switched on nationwide or partial NB IoT Networks in 114 countries[9]. The number of devices already connected on NB IoT is predicated to be around 187 million, and this is projected grow at exponential rates in the upcoming years[10].

The Opco's Implementing smart access control solutions have the potential to touch almost every aspect of their company, in particular their profits, bottom line and their relationships and agreements with enterprise customers. This section of the report will consider the impact of smart access on OpCo's from the context of:

- Narrowband IoT product/services business models
- Existing large enterprise customers 'smart wants and needs'
- Security and compliance



Graph above: Number of NB IoT devices installed globally

NB IoT Products/services business models

OpCo's can choose from four basic business models for adopting NB IoT products/services as according to their strategy per country or region. These models are outlined below:

Model 1. Connectivity only: For NB IoT devices, reliable connectivity is required and can be charged to the device manufacturer or end customer.

Model 2. NB- IoT as a service: software/platform solutions with predictive analytics, AI, machine learning, security, billing, big data integration and quality of service assurance can be offered to customers supporting the global trends of network/data virtualization and cloud-based service provision.

Model 3. End-to-End (E2E) 'smart service' provision: OpCo's can choose to go further up the value chain by taking over more responsibilities than pure connectivity/service such as offering customer management, and system integration functionalities providing the tools to exchange the data and knowledge. The OpCo can also outsource certain parts of the E2E domain to its partners, sharing effort and revenues, whilst at the same time expanding the operators own experience and opening new opportunities in the Over The Top (OTT) domain.

Model 4. End-to-end 'smart device' provision; OpCo's can choose to sit at the top of the value chain, by adopting their traditional business model of purchasing hardware (like mobile phones) and upselling with connectivity on 1,2, 5 or 10 year 'plans'.

With NB IoT the traditional OpCo 'mobile phone model' simply changes out the 'mobile phone

[9] https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

[10] https://www.iot-now.com/2018/07/04/85156-nb-iot-networks-now-time-make-business/

hardware', with 'smart device hardware'. This model does not necessarily mean that sales of smart devices should occur in retail stores, although this seems beneficial to the Opco. This model should also be focused on satisfying demand with existing large enterprise customers, and using the model to attract new enterprise customers. This model can be particularly useful for OpCo's to satisfy the existing enterprise customer who already has placed significant trust in them.

Assessment summary for adoption of NB IoT Smart Access for Telecommunication company's

Smart Access control offers the OpCo the opportunity to choose the implementation a variety of the above business models. When considering big data, the business model opportunities are even more greatly enhanced.

Devices with simpler functionality such as pet trackers/kid trackers lend themselves to simpler business models such as only adopting business model 1 discussed above. In this tracking case, the customer is usually a consumer and not an enterprise, and the potential to integrate additional products and services to the tracking device is limited.

The greatest value to the OpCo, when it comes to adopting NB IoT smart access control, is model number 4. NB IoT smart locks can be bought from a manufacturer and invite large margins which exist in the access control industry. In addition, bundling opportunities with other IoT products are enormous.

Further by adopting business model 4, the traditional OpCo model, Smart Access systems can offer the opportunity for OpCo's to reduce the risk of losing large enterprise customer accounts by supporting the enterprise's desire to improve its management and cyber security features. Further the OpCo can also encourage even more efficiencies to their enterprise customers for further adoption of other NB IoT smart device products and services in the future.

As the rollout of 5G occurs across the planet, high data plans and devices can also be offered to the enterprise customer and bundled together on the same 5G IoT platforms that NB IoT is a part of.

Existing large enterprise customers smart demands

A major portion of telecommunication products, equipment and technologies are intended to facilitate customer choice and control with regards to their communications.

This should also include offering or at least supporting, the implementation of products, services and tools that enable large enterprise customers to better manage their machine to machine/cloud communications.

A successful smart building implementation that has a focus on the customer will rely heavily on customer participation to achieve increased security, efficiency, utilization, and customer satisfaction.

Under this scenario, existing telecommunication large enterprise customers are constantly demanding and wanting to participate in the following 'smart' behaviors to improve their building and organizational management efficiency:

- have access to and regularly evaluate their security and access profiles, patterns, and trends
- Adjust their key management patterns and practices to minimize their costs and optimize staff time efficiencies.
- Invest in other 'connected' security and access control products that can respond to price reductions, such as self-monitoring intruder alarms, door open too long alarms, self-monitoring CCTV.
- Reduce building energy consumption and energy costs, also known as 'smart energy management' such as installing smart thermostats and smart lighting.
- Participate in other building related health, safety and environment improvements with connected 'smart' sensors, such as preventing fire outbreaks, managing water usage, and noise detection
- Have access to a central cloud IoT platform, which is secure, scalable, and manageable, enabling all data from a variety of IoT products and services to be

captured and analyzed in one platform. A strong IoT platform can respond, adapt and optimize building and organizational management in new innovative ways.

There are means for large enterprises to accomplish many of these above 'smart' behaviors on their own; however, smart building products/services, and the communications between them require telecommunication company involvement.

For example, a customer may purchase a typical RFID keycard system and have a local locksmith install it. Under current conditions, with closed offline systems, the security and access of the building will be improved, but desired behaviors such as remote distribution of digital keys to mobile phones to save time and money, in addition to live notifications and live audits of lock activity, crucial for data analytics, will be lost.

In this example above, the enterprise does not get a taste of data analytics, and the benefits this can bring, so they are not motivated to explore other new 'interfacing' smart products. A connected NB IoT lock, with its unique features, and the data it can capture, in addition to the other products and services it can integrate to on one platform can inspire the large enterprise to invest in other NB IoT (and 5G) products in the future.

In addition, without telecommunication coordination, education, support and incentives, it has been demonstrated that only an extreme few enterprises will be willing or capable to take the steps necessary to manage their machine to machine operations and communications effectively on their own.

Finally, the OpCo also does not want their existing large enterprise customers to turn to building their own unlicensed and insecure Low Power Wide Area networks such as Lo-Ra and Sigfox for their machine to machine communications. These networks have proven to be difficult and costly to build (e.g the private operator must install telecommunication equipment on their own towers or buildings or get permissions to install on other buildings).

OpCo's have invested heavily in building out their secure networks, and more recently increasing their investments into NB IoT and 5G, and so to see a return on their investment, it seems prudent that they look to an industry like access control to disrupt.

Implementation of smart connected devices and software, along with new networks often create new sensitive data and vulnerabilities. This data may consist of critical company operational data and sensitive customer usage information. Both types, if left unprotected, can result in reliability and privacy risks if exposed. OpCo's can offer a robust cyber security strategy to enterprise customers to accompany smart access implementations of smart devices and software. This strategy should address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent exposures due to user errors, equipment failures, and natural disasters.

In summary, it would be a "waste" of the OpCo's investment in NB IoT and 5G, if they cannot make available their secure established networks for widespread use in the physical security industry.

Recommendations

This business case analysis has provided an overview of the access control market and identified a number of opportunities the OpCo can consider to improve revenue opportunities, retain enterprise customers and gain new ones, establish NB IoT as a new standard in the security/access control/smart building market, and explore 'Over The Top data analytics' business models and opportunities.

Based on the quantitative and qualitative results of this business case analysis, we have identified the following notable observations and recommendations for OpCo's:

- NB IoT Smart Access control has the potential to provide OpCo enterprise customers with significant benefits in the form of improved security, cost and time savings, meeting regulatory and compliance requirements, tracking employees, and exploring data analytics to improve management efficiencies.

- OpCo's do not need to make any significant financial investments to take advantage of the opportunities NB IoT smart access offers other than continual

learnings of the smart product devices and the industry they exist in.

- NB IoT smart access can act as the 'trojan horse' for OpCo's enterprise customers to adopt NB IoT as part of a longer-term smart building strategy. In the future, after adopting the first NB IoT product, such as NB IoT smart access, the enterprise can more easily be offered other products and devices built on NB IoT.

- OpCo's can offer to their enterprise customers a cyber security threat and vulnerability evaluation/gap analysis with a cyber security strategy to address or mitigate known risks. NB IoT can be a central part of this analysis.

- The Opco can choose a number of business models to capitalize on the NB IoT smart access control opportunity and are not limited to simply selling SIM's and connectivity.

- OpCo's should begin placing greater emphasis on educating existing enterprise customers and personnel about the ongoing challenges and emerging opportunities in the security, access control and Internet of Things industry. The future of the Internet of Things industry and customer interests are expected to evolve to a more complex environment that will require robust data-centric infrastructure. As such, OpCo's should begin to gauge customer interests in adopting NB IoT technology now such as having access to data (through one central web portal), and offer savings potential in management behavioral changes.

- Evaluation of future smart building devices that can be converted to NB IoT should immediately be explored by the OpCo, and investment should be made in the development of a diverse and robust portfolio of smart building products, that could be aggregated into a fully integrated system, as they can bear significant value potential.

- NB IoT has the potential to become the new security/access control industry standard by offering a large range of functionalities that have never been able to be offered to customers before.