DIGITAL KEYS

5G IoT SMART ACCESS CONTROL

Business Case

Contents

1.0 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 online technologies and the **Internet of Things(IoT)** into the traditional electronic keycard access control system to deliver more efficient, more secure and more responsive services to customers.

When adding wireless internet connected technologies such as Wi-Fi and Bluetooth and their related processes to access control, the terms "**smart locks**" or "**smart access**" or "**smart access control**" are used.

Whilst '**smartcard or keycard'** access control has been around for about 30 years, it should not be confused with **smart access control.**

Smartcard/keycard 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 'time-sensitive' digital key unlocking, remote unlocking, live audits and notifications, instant cancellations of digital keys, and big data analytics and more.

The speed of smart access adoption in enterprises 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 internet connected[1]'.

The slow adoption rates of smart access can be attributed to higher costs of wireless products, unreliability of wireless technologies, difficulty in setting up the products, and the need for significant onsite network infrastructure (such as Wi-Fi mesh networks).

But one of the main reasons 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 been exposed in recent times as "hackable" and "insecure".

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 '**connected cyber insecure'** times.

What the physical security industry needs now is a **new communications technology** to meet all the challenges it currently faces.

Smart access control demands a technology 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. This technology has recently been launched and it's called **5G IoT.**

2.0 Definitions

TERM	DESCRIPTION
IoT	Internet of Things, a generic term for the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. In short it is about the extension of internet connectivity into physical devices and everyday objects.
5G IoT	Refers to low power wide area (LPWA) 3GPP/GSMA standardised secure operator managed IoT networks in licensed spectrum. In particular, networks designed for IoT applications that are low cost, use low data rates, require long battery lives and often operate in remote and hard to reach locations. 5G IoT networks include LTE-M networks and NB-IoT networks (see definitions below)
LTE-M	The industry term for the Long-Term Evolution (LTE) machine-type communications (MTC) LPWA technology standard introduced by 3GPP in Release 13. LTE-M supports lower device complexity, massive connection density, low device power consumption, low latency and provides extended coverage, while allowing the reuse of the LTE installed base. The deployment of LTE-M can be done “in-band” within a normal LTE carrier, or “standalone” in a dedicated spectrum.
NB-IoT	Narrowband-IoT is a 3GPP radio technology standard introduced in Release 13 that addresses the LPWA requirements of the IoT. NB-IoT is characterized by improved indoor coverage, support of massive number of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimized network architecture. Like LTE-M, NB-IoT can be deployed “in-band” within a normal LTE carrier, or “standalone” for deployments in dedicated spectrum. Additionally, NB-IoT can also be deployed in an LTE carrier’s guard-band.
5G-IoT commercial launches	The first **5G IoT commercial launches** were completed in 2016 and a global roll out has been underway over the last few years with over 100 Telecommunication companies now adopting 5G IoT on their mobile networks, with full nationwide coverage in around 80 countries, with partial nationwide coverage in 74 other countries[1]. The 5G IoT networks are software upgrades on existing 3G, 4G and 5G networks and do not require any new equipment installations.
IoT Market	The **IoT market** is expected to be bigger than the smartphone, tablet, and PC markets combined, expecting to double by 2021 to $520B[2] with connected locks sitting at the top of projected IoT device sales over the next five years.

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

1.1 [2] *NCTA -The Internet & Television Association, Washington DC, USA

3.0 Smart Access

WHAT IS SMART ACCESS?

Access control is defined simply as ‘the selective restriction of **access** to a place or other resource’, whereas **smart access control** or simply **‘smart access’** is generally defined as a combination of ‘traditional access control’ (i.e. with keycards/software or metal keys), with ‘**smart controls via the internet**’ (e.g with cloud-based software, smartphone apps with digital keys, data analytics).

Smart access is about more than just security – it 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 is about delivering security, controlling access to assets/buildings, and more efficient key management leading to cost and time savings.

From a customer ‘end-user’ perspective, smart access offers more convenient access, safety /security, and peace of mind.

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

The access control industry has obviously always been concerned with security, but in more recent times, the industry has had to think about cyber security and 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.

4.0 Smart Access Motivations

Companies need to meet specific sets of mandatory regulations to ensure a safe and secure workplace. Smart access control can help meet a lot of those regulations, especially around the ‘protection of company resources against unauthorized access’. But there are also many other specific industry motivations for smart access control.

SMART ACCESS CONTROL FOR THE HEALTH INDUSTRY

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 FOR THE FINANCIAL INDUSTRY

In the financial services industry, smart access control can help 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. Internally, most staff must also be restricted to access certain rooms that house computers/servers with 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 – so a record is kept of who opened which door at what time.

SMART ACCESS CONTROL FOR THE SOFTWARE INDUSTRY

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 CONTROL FOR MANUFACTURING AND INDUSTRIAL SECTOR

Regarding **staff safety, manufacturers (and other related industries) have a responsibility to ensure the health and safety of their employees around equipment** and they must set 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 at all times, and the work environment must be secure and safe. For example, in most manufacturing environments the general public should not be able to roam around floors with machinery, 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, and for insurance reasons.

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', with the lock sharing information (not the user's mobile phones) recording in a cloud database who opened which door at what time (and also providing live text/email notifications to managers.

SMART ACCESS CONTROL FOR THE REAL ESTATE INDUSTRY

Real Estate Agents who often manage thousands of properties, can use digital keys instead of metal keys for better management and efficiencies. For example a RE Agency 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 hunters time to roam throughout the house, and leave.

SMART ACCESS CONTROL FOR THE LOGISTICS INDUSTRY

For employees that need to access multiple sites on a regular basis, such as workers of utility companies, or postmen/courier contractors/delivery people, 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 to head offices.

SMART ACCESS CONTROL FOR THE ACCOMMODATION INDUSTRY

Hotel managers can know what rooms staff and guests are going into at anytime for security and safety with live audit notifications/record keeping in the cloud-based software. **Guests** can be offered self-check-with digital keys, bringing greater satisfaction in not having to line up, or to chase down metal keys from hotel managers after hours, especially in small independent hotels only open 9am-5pm.

SMART ACCESS CONTROL FOR THE INDUSTRIES THAT CAN BENEFIT FROM DATA ANALYTICS

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 and as technologies such as 5G and 5G IoT advances. 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.

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 FOR THE OFFICE INDUSTRY

The Office Industry looking to improve their current access control so as to protect server rooms, and improve sharing of meeting rooms. They're also looking for seamless ways to provide shared temporary use of office spaces, like meeting rooms and shared labs like Airbnb does with accommodation.

5.0 Smart Access Technologies

ARE THEY SECURE?

The technologies currently used in smart access control include only a small handful such as Wi-Fi, Bluetooth, Zigbee, and Z-Wave. These technologies were originally designed mostly for human connections and not machine to machine connections/machine to cloud connections. As a result, these technologies are often "hacked", antiquated, fragmented, non-standardized and insecure.

The shortcomings of smart access control technologies currently available in the marketplace include;

- ✓ poor reliability
- ✓ high operational and maintenance costs
- ✓ high set-up and infrastructure costs.
- ✓ Low battery life
- ✓ Poor connectivity/integrations across platforms and devices 'e.g devices not playing well with others'
- ✓ Difficult in setting up devices
- ✓ Poor security

With poor security, for example, in October 2017, a massive security vulnerability called KRACK, effected Wi-Fi devices and Wi-Fi smart locks. The KRACK hack allowed hackers to hijack your Wi-Fi connection, inject content, steal passwords, and monitor your traffic.

Enterprises customers are demanding smart access control with detailed attention to 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.

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

As a result of the significant global apprehension and publicity around cyber security and its relation to "internet connected" smart access control systems, the only way to overcome this fear is to offer a new more advanced technology for smart access such as 5G IoT.

A summary table is included below of some of the recent hacks/insecurities of existing access control technologies currently available in the marketplace.

TECHNOLOGY	HACKING/INSECURITY DETAIL
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
ZWAVE	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 5G IoT CAN ADDRESS CYBER SECURITY ISSUES

Unlike most forms of internet connectivity, 5G 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.

5G IoT has passed security protocols as outlined by 3GPP, and the GSMA, the organisations responsible for managing the mobile networks. 5G IoT is designed for global use in machine to machine and machine to internet/cloud communications, and it is the only licenced technology for these purposes.

To meet licencing approvals, numerous regulatory schemes from governments such as the FCC (USA) must be met, in addition to passing strict testing, compliance and enforcements from many other certifying bodies too. All other unlicenced machine to machine/IoT communication technologies such as Lo-Ra, Sigfox and others are unregulated, uncontrolled and insecure.

By supporting an array of security features and safeguards 5G 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.

Over the last 20-30 years, mobile operators and public cloud operators have spent billions of dollars building security features and safeguards into their mobile/IoT networks and public clouds. Some of these security features are outlined in the table on the next page.

> “5G IoT Smart Access Control helps prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information.”

Table 2 – Security feature examples built into 5G IoT smart devices

SECURITY FEATURE LOCATIONS	FEATURE DETAILS
Between telco mobile network and device management platform	A layer of Internet Protocol Security (IPSEC) is provided.
Between telco mobile network and device manufacturers IoT cloud platform	A dedicated VPN is provided
Between device and IoT cloud platform	The device that sends data to the cloud is authorized and so it cannot be replaced/altered with by another.
Between device and IoT cloud platform	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
All layers	All communications are running on HTTPs military grade 128-256-bit encryption including on all vertical layers between software and hardware, plus 2048 bit IoT chipset encryption
All layers	The encryption of all data in transit uses 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 and Transparent Database Encryption (TDE) is enabled
All layers	Meets OWASP Top Ten (the Most Critical Web Application Security Risks).
All layers	Does not use open source components and supports IP whitelisting
Cloud IoT platform layers	Meets vulnerability/penetration testing such as having SSL certificates/wildcard certificates and supporting large enterprises existing certificates.
Cloud IoT platform layers	The systems uses secure infrastructure to download automatic updates and updates are validated before they are installed.
Cloud IoT platform layers	Monitoring for data tampering and integrity takes place and the application alerts the user if any suspicious transactions are found.
Cloud IoT platform layers	Cryptographic keys are stored securely and managed throughout their lifecycle. Access to the keys are restricted, audited and logs retained
Cloud IoT platform layers	Platform is hosted at a server farm locally (in countries where the devices are located) and certified to meet certain Government regulations.

6 .0 Smart Access Adoption

To date, adoption of smart access control systems has been very low, and hardwired systems still have an edge. 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.

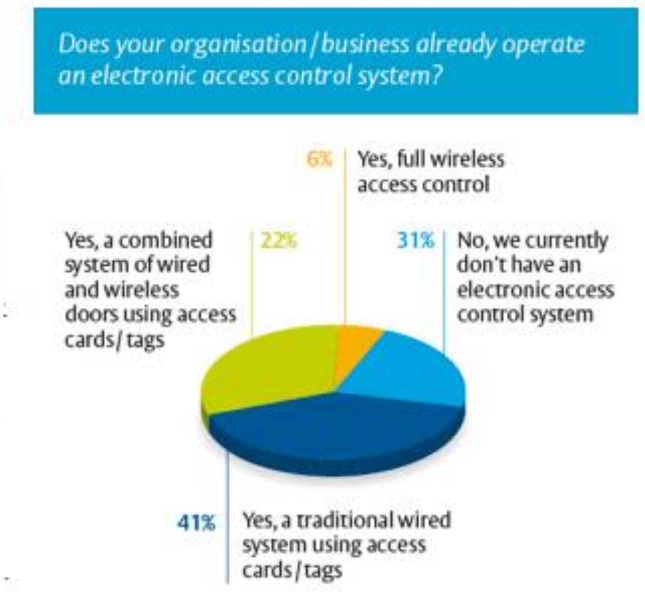
Impediments for companies and organizations to move ahead with transformation to a smart access control system, in addition to cyber security fears discussed in the previous section, include;

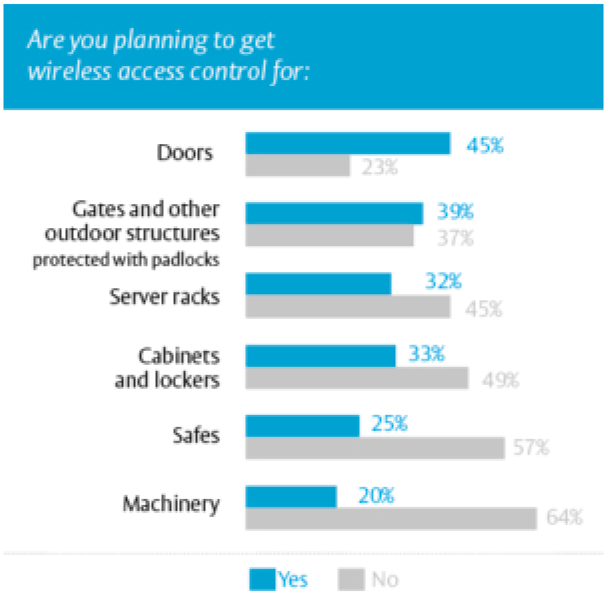
- ✓ Fears of new technologies
- ✓ Skepticism regarding benefits as compared to costs
- ✓ Resistance to change
- ✓ Building trust in the parties delivering the product and services (e.g public cloud provider, device manufacturer, IoT network operator)
- ✓ Having a mixture of technologies in building management devices is too difficult - for example if you have Wi-Fi/BLE smart locks, it can be hard to get them integrating with Z-Wave burglar alarms, and with wired smoke alarms and CCTV systems.

In 2019, an Access Control Trends Report[3] by HID Global (a leading American manufacturer of secure identity products) interviewed hundreds of professionals involved in the procurement, operation, deployment or maintenance of access control systems, to gauge perceptions of, and demand for, wireless technologies. The report revealed only 6% of installed electronic access systems are fully wireless/internet connected. 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.

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

One of the reasons for low adoption rates for smart access can be attributed to higher costs of existing wireless access control systems, commonly built on Wi-Fi/BLE, as compared to their wired counterparts. Wi-Fi/BLE systems are generally more expensive 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 from qualified technicians.





ADOPTION OF "NON-DOOR" SMART ACCESS

Survey data from the HID report highlighted the growth potential of smart 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.

INCREASING ADOPTION OF SMART ACCESS

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

Mirroring the usual trajectory of emerging technologies, smart access control systems over time are becoming less expensive, more reliable and more versatile. Nearly two thirds (63%) of respondents in the aforementioned HID survey "have a more positive view of smart access than five years ago because the technology has improved".

Interoperability is critically important for any enterprise investing in new or upgraded access control systems and so smart access is often seen as 'the next natural step'. Enterprises need to plan for eventualities they may not even see yet. Ending reliance on a single, proprietary offline wired solution will make access control more flexible for future uses. With smart access for example, you can add a new building, and bring its access control into the existing cloud-based system seamlessly in minutes. Procurement decisions should be made with the long term in mind. For buyers and manufacturers, the future is now.

The enterprise embracing 5G IoT smart access control realizes new smart building products will continue to be developed in the future with 5G/5G IoT technologies, and these products can easily be interfaced onto the one cloud-based platform. Smart building systems and devices can mature and confidently 'grow together' without the risks of hacking. For example, a 5G IoT alarm system can easily integrate immediately and automatically 'out of the box' to their existing 5G IoT smart access control system without having to do any complicated set up.

5G IoT smart access control can even be integrated into legacy devices and systems and elevate older 'disconnected' systems for better efficiencies and building management. For example, if you have an existing offline RFID keycard system in your building, you can install 5G 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 currently operated by a metal key, can become connected with 5G IoT and the gate digital key can be added to the NFC sticker too and stuck onto the workers RFID keycard.

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 management system'. This 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.

SMART ACCESS AND BIG DATA ANALYTICS

Enterprises adopting smart access can be introduced and educated about a lot of the hidden values that connected systems bring to their enterprise such as **big data analytics**, so they will constantly demand other smart products and services built on 5G IoT technology in the future.

Smart access system represents a unique opportunity for enterprises to get a taste of big data analytics, automations, and predictive AI, with all their associated benefits. For example, enterprises can start with adopting 5G IoT smart access control and build an appetite for further adoption of other smart buildings products/services such as 5G IoT smart electricity metering, 5G IoT smart parking, and 5G IoT smart lighting and more.

The improved data management that comes with 5G IoT smart access also 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.

To meet their requirements for smart access control, enterprises demand management system architecture/hosting that is cloud-based, SaaS style, with the underlying infrastructure operated, managed and maintained by a trusted company such as a telecommunications company, or companies with strong cloud services. Cloud-based 5G IoT smart access control meets the following requirements for enterprises as outlined in table 3 over the page.

Table 3 What enterprises demand of smart access systems

REQUIREMENT	DETAILS OF REQUIREMENT
Hosting and management of the cloud-based platform is through a single administration portal	It does not rely on multiple consoles, so there is no need for onsite infrastructure, and the system can be managed from anywhere.
Smart Access Management Software uses Active directory-based authentication	This is for administration users and role based access
IoT platform, software and mobile apps synchronize with the Active Directory on a regular basis	This ensures access is removed from the application in a timely manner once a user's account has been disabled, and/or after the time for their approved access expires.
Software has alerts and notifications directly to operator/account administrator	If an access control device is unavailable, has low battery, or is being tampered with.
Software has mapping	A map shows of all the enterprises buildings/assets and the location, health and status of the access control devices and are interactive
Smart Access Management software is public cloud-based	The public portal (website log-in/mobile app) is for external users to register for new accounts and for access to select buildings/rooms/assets from anywhere in the world
Software can be used to create time-sensitive digital keys	A list of rooms/assets are stored for the users to select from to create time-sensitive digital keys, and to remotely unlock.
A mobile app is available to download from online stores	The issue of credentials (unlock button) to a user's mobile device is immediate (within 2-10 seconds)
Software records events and sends live notifications of events (audits)	The usage of the system is audited and allow administrators to get reports of any user or activity at anytime through notifications, texts, emails etc.
Software is intuitive and provides an easy-to-use user experience	Its flexible and works all hours/outside of normal business hours
The solution does not introduce any additional overhead and latency onto the enterprises systems	User productivity is not affected
The solution offers automatic update policies, controls and new mobile app versions	Doesn't connecting directly to the enterprise's network
IoT cloud provider guarantee near 100% availability of any cloud component of their solution.	The system architecture is fully documented and includes all system components, ports, protocols, interfaces, etc
The software allows the enterprise to produce reports for compliances	Downl oad/export audit logs as CSV files for use in spreadsheets and databases, and data analytics
The solution allows for secure API based integrations with standard, open protocols that supports the use of an application proxy that brokers the connection between the cloud.	Interfaces 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. The API's should not store data temporarily on disk to facilitate the transfer of data between applications.

7.0 Conclusions

Beyond the inherent security built into mobile networks using the 3GPP standards which 5G IoT smart access control systems take advantage of, public cloud providers are also providing an array of additional security features and services for Internet of Things devices.

As regulated entities with spectrum licensees, mobile operators also have to comply with a range of requirements established by the regulatory authorities in the markets in which they operate. In most countries, mobile operators now have long track records of keeping their networks secure, building trust among regulators, governments and policymakers.

As a result, 5G IoT smart access can provide both consumers and companies with connected access control that is far better protected than smart access control built on Wi-Fi/Bluetooth and other technologies that have been hacked, and are insecure and unreliable, and which require complicated setups and a lot of supporting equipment.