NB-IoT™ Smart Access Control Fact Sheet

For Workplaces

What is NB IoT?

NB IoT is a new communications technology which enables devices to connect to the internet with improved connectivity, less energy expenditure, greater reliability and greater security. NB IoT is also a purpose-built network for machine to machine operations, meaning that Wi-Fi and Bluetooth, built for human operations, can be eliminated. NB IoT is built on telecommunication companies existing mobile networks, and is currently live in 33 countries, supported by over 30 of the world's largest mobile operators, culminately worth over $660 billion, who provide communications to over 2.9 billion customers and geographically serve over 90% of the IoT markets in 79 countries.

Why is NB IoT used in Access Control?

The humble **metal key** has been used to secure properties, spaces, and assets since the Roman days over 2000 years ago. In the latter half of the 20th century keycard systems, commonly found in hotels and offices were invented to provide **access** to a variety of people for different time frames, and to **control** what rooms or spaces those people can access. Hence the **access control** industry was born. These keycard access control systems need to have people managing/programming them, and communicating with them. This communication was originally done by wiring all the locks together, and connecting them to onsite servers and PC's, and large controller boxes to house all the electronics.

When the internet came along the wiring used in the keycard access control systems was able to be replaced by Wi-Fi, Bluetooth, Z-Wave, and other communication technologies. This opened access control, originally limited to hotels and offices, to places such as people's homes. It also introduced smartphone digital keys, reduced costs, and spawned a new product and industry called **smart locks.** But the problem with these smart locks is that they still require onsite network infrastructure, and onsite electricity to run. And each different location has its own unique network, making it hard to bring multiple smart locks together under the one control system. Also Wi-Fi, Bluetooth and other communication technologies that the smart locks used, have proven to be hackable, and unreliable for access control. A new technology solves all these problems, and its **called NB IoT.**

What is NB IoT Smart Access Control?

NB IoT Smart Access combines smart locks, with keycard access control, but instead of using onsite network infrastructure everything is inside the lock, and the rest of the infrastructure is in the mobile network. In short, it's like **making a lock like a mobile phone** with its own little modems, little computers, antenna's, apps etc.

Why should workplaces get this?

Track/monitor employee's presence on sites in real-time for mandatory Occupational Health and Safety reporting/legalities, and for emergency and insurance situations with live audits to administrators' phones. Those companies/businesses that do not meet OH&S guidelines (regarding tracking can be fined or liable to legal action). The smart lock can become like a punch card log in system.

Improve security and convenience by distributing digital keys online for limited time periods and making them easily self-accessible to so that workers/contractors/visitors can be controlled access to certain offices, storage rooms, server rooms, lunch rooms, meetings rooms etc.

Save money by not having to pay a locksmith $150 to replace locks after a metal key is lost/not returned - if anyone finds the metal key, or copies the metal key, the security of the building is compromised and anyone can give themselves unauthorized access at anytime.

Save time and money managing metal keys for workers to access multiple properties, spaces etc. For example if you have many shops with workers always moving around, then it can take 10 seconds to generate a time-sensitive digital key, or one-time digital key and distribute it to workers phones.