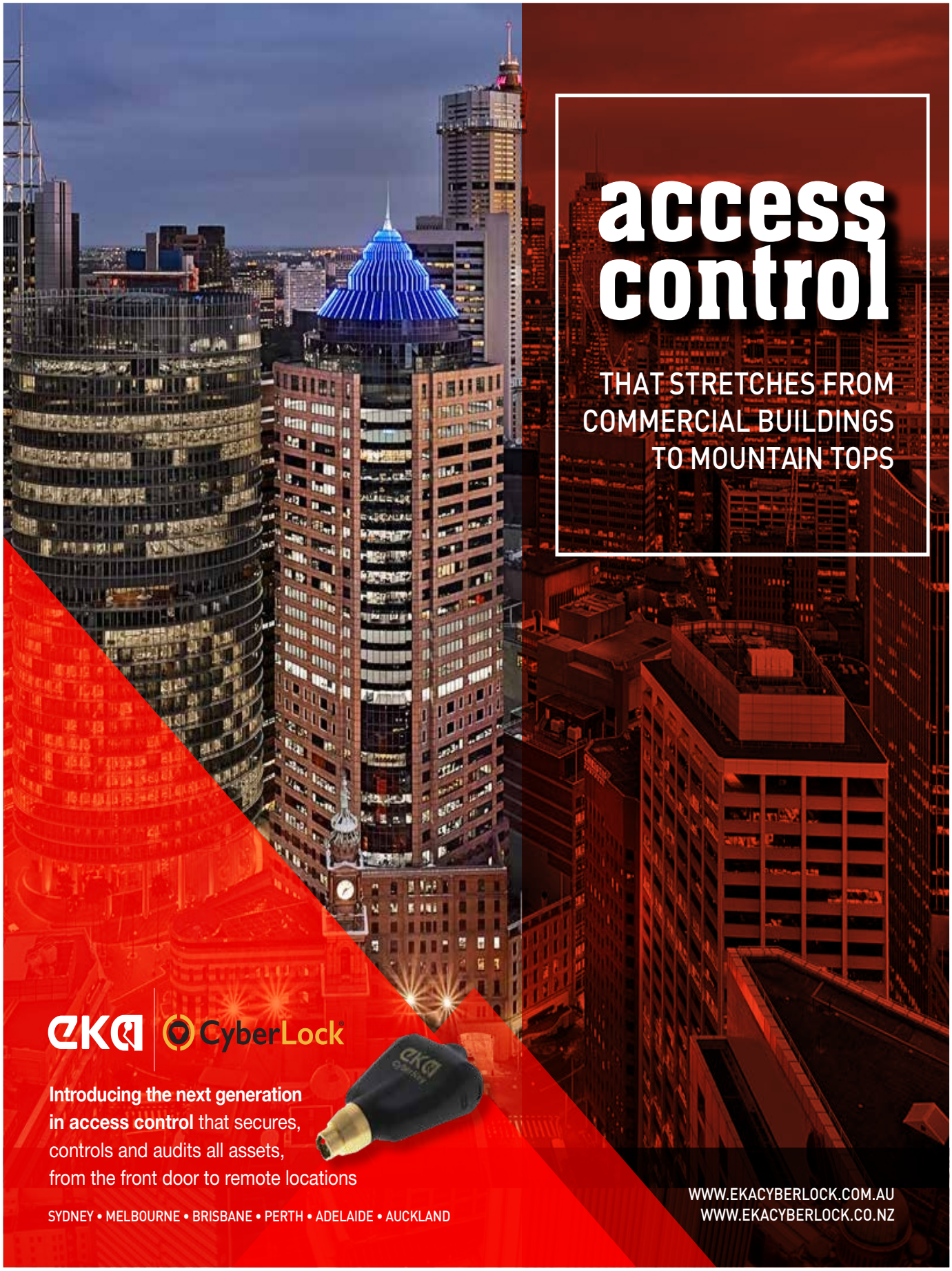

access control
THAT STRETCHES FROM COMMERCIAL BUILDINGS TO MOUNTAIN TOPS
EKA | CyberLock
Introducing the next generation in access control that secures, controls and audits all assets, from the front door to remote locations
SYDNEY • MELBOURNE • BRISBANE • PERTH • ADELAIDE • AUCKLAND
WWW.EKACYBERLOCK.COM.AU
WWW.EKACYBERLOCK.CO.NZ

ABOUT

EKA CYBERLOCK

Introducing the next generation in access control that secures, controls and audits all assets, from the front door to assets in remote locations.

WHAT IS EKA CYBERLOCK

EKA CyberLock is an electro-mechanical master key system. It is a hybrid product that has combined the attributes of conventional proximity or swipe card access control with those of a mechanical master key system.

With an EKA CyberLock system, it doesn't matter where the lock is, electronic access control is possible.

By eliminating the wire between the lock and the managing software, EKA CyberLock can be installed virtually anywhere. The convenience of a mechanical key system plus the access permission and tracking capability of an electronic access control system come together with EKA CyberLock.

Securing an office door with current access control technology is easy. However, conventional cabled access control is not practical for controlling access to remote assets, like sub-stations, data centres, vending machines or even the service rooms of large buildings.

EKA CyberLock finally breaks this either/or choice. EKA CyberLock couples the master-key ability to put a lock on anything with the tight and trackable access control characteristics of swipe card systems.

What's more, EKA CyberLock retrofits into most existing locks and complements any existing access control system by extending your control to virtually every door.

That's why EKA CyberLock truly is the next generation in access control — able to secure, control and audit any asset from an office door to remote or mobile assets.

EKA CYBERLOCK 4 MAIN COMPONENTS

CyberKeys
The CyberKeys are used in a similar way to a conventional key except that the CyberKey has no cuts. It is 100% electronic, programmable and is loaded with the access profile of the key owner.

CyberLock Cylinders
CyberLocks are the electronic lock cylinders. They are the same dimensions as the mechanical cylinder which they replace and are suitable for doors, cabinets, padlocks and virtually anywhere a CyberLock is currently installed. The cylinders require no permanent wired power as they are powered by the battery in the CyberKey. The CyberKey has an access profile, and if the profile includes the permission to open a specific cylinder then the cylinder can be turned to open in a similar way to any conventional key lock.

CyberAudit Software
Available in self-hosted or fully supported cloud applications. The software is used to configure and manage the system, providing control of all access profiles, users, CyberLocks, CyberKeys and auditing functions.

Communicators
The EKA CyberLock system has no wired connection to CyberLock cylinders or CyberKeys. Communicators provide the ability for the software and the CyberKeys to communicate. There are many forms of communicators and these include 20 key vaults, key pad authorisers and even mobile apps that communicate with CyberKeys via a smartphone and Bluetooth.

Combined, these four main components form a fully functional access control system. However, it's an access control system with some distinct advantages. It goes beyond the door and can be incorporated into virtually anywhere a lock can be installed such as padlocks, server racks, camlocks, portable applications and even remote sites, all without cables or power to the lock.

CYBERKEY

SMART KEY

The CyberKey is an electronic, programmable smart key that cannot be duplicated.

List Of Available Keys

- CyberKey II Rechargeable
- CyberKey II Battery
- CyberKey Air
- CyberKey Blue 2
- CyberKey Plus
- CyberKey Flash

Each CyberKey can be programmed with the permissions for every CyberLock: which CyberLocks a users CyberKey can open, as well as the days and times each CyberLock can be opened.

In this way, each user only needs one CyberKey to access any CyberLock in a system, whether it's a major entry door, or an obscure and remote cabinet or padlock.

Since the CyberKey is electronic, permissions can be revoked. Administrators can set CyberKey expirations to occur regularly (daily, weekly or more often) and can also do this on an ad-hoc basis if CyberKeys are lost.

Each CyberKey contains four levels of intelligence: encrypted access codes to ensure the key is from the same installation; the unique ID number of the CyberKey; access privileges for the user of the CyberKey; and storage of up to the last 12,000 events, both entries and denied entries.

The unique exchange of encrypted access codes between the CyberLock and CyberKey gives the highest degree of key integrity. The encrypted codes ensure CyberKeys from other systems cannot work in your system.

PERMISSION & SCHEDULES

Each CyberKey contains a specific list of authorised CyberLocks and a schedule of when they may be accessed.

For example, a CyberKey can be programmed to allow access to one or several CyberLocks from 8 a.m. to 6 p.m. on weekdays and 10 a.m. to 4 p.m. on Saturdays. CyberKeys presented outside of this schedule are denied access.

All user CyberKeys can be programmed to block other user CyberKeys in the event of a CyberKey being lost or stolen.

CYBERKEY EXPIRATIONS

CyberKeys can be assigned a start date and an expiration date. This means CyberKeys can be issued before they become active, and can be set to expire at a specific time in the future.

Administrators must authorise CyberKeys before access will be granted again.

Setting short-term expiration dates is an excellent way to minimise risk due to lost or stolen CyberKeys.

SMART KEY FEATURES

- Standard, rechargeable, Bluetooth and Wi-Fi versions available
- Contains a unique ID that cannot be changed or duplicated
- Has the ability to store thousands of access records: Lock ID, Date & Time, Event Type
- Carries access schedules for the specific key holder
- Retains encrypted access codes that bind the key to a specific system
- Includes a battery which energises both the CyberKey and each CyberLock it touches
- Includes rechargeable key options or CR2 lithium battery
- Non-volatile memory holds access events, even if the battery fails
- Made from impact-resistant nylon for high durability
- Water-resistant, coated electronics
- Sacrificial brass tip prevents wearing of CyberLock cylinders
- Brass tip easily replaced in the field
- Can be programmed for one or many CyberLock cylinders
- Multiple notifications (beeps, flashes or even email notifications) for low battery on CyberKeys

CYBERKEY

BLUE 2

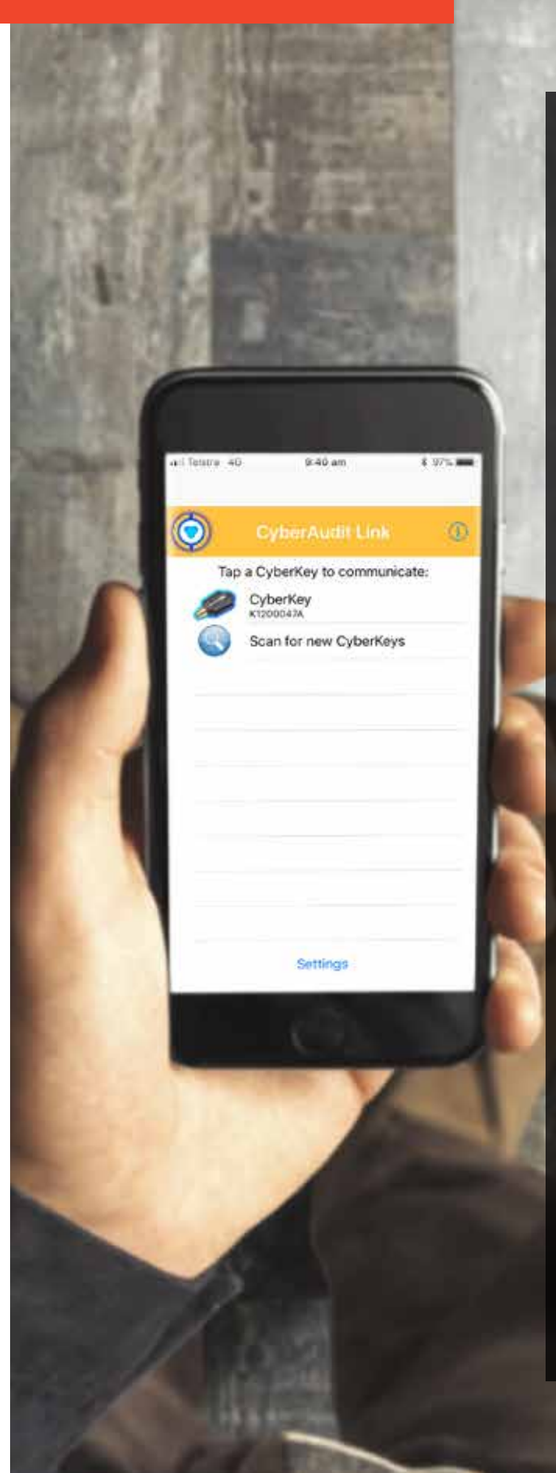
The CyberKey Blue 2 is a second generation bluetooth electronic key used to operate CyberLock electronic cylinders.

The CyberKey Blue 2 via a smart device app enables each user to activate & deactivate a CyberKey in-situ, as well as communicate with EKA CyberAudit-Web management software.

The fact that the CyberAudit Link app communicates with the CyberAudit-Web means real time audit reporting and instant reassignment of access permissions.

Permissions are updated via the CyberAudit Link app to the CyberKey Blue 2 when in a mobile network coverage area or connected to Wi-Fi. If in the instance, an opening of a CyberLock cylinder is in an area with no mobile network coverage, then the CyberKey Blue 2 already contains the permissions, thus allowing delayed activation. Furthermore, users don't need to open the CyberAudit Link application to deactivate their CyberKey Blue 2; however, for high security or sensitive environments, the CyberKey Blue 2 can be deactivated by the user.

Like all CyberKeys, CyberKey Blue 2 can be programmed to be activated and deactivated for a specified period of time. It has non-volatile memory that contains encrypted access codes, a list of CyberLocks it may access, schedules of dates and times it may access CyberLocks and a begin-end date range during which the CyberKey will operate.



CYBERKEY BLUE 2

WITH BLUETOOTH 4.2 WIRELESS TECHNOLOGY.

DUAL MODE, CLASSIC OR BLUETOOTH LOW ENERGY

ULTIMATE CONVENIENCE

Pairs with Smart Devices running the CyberAudit Link App

GREATER FLEXIBILITY

Individually manage fully customisable permission schedules

CONTROL

Reports audit trails within seconds for accurate record keeping

DELAYED ACTIVATION

Delayed activation for remote locations without mobile network coverage

EXPANDED MEMORY

Contains encrypted access codes and records up to 12,000 audit trail events

COMPATIBILITY

Android and iOS compatible

ELECTRONIC LOCK

CYLINDERS

The CyberLock cylinders are the exact dimensions of the mechanical cylinders they replace. They are an electronic version of a standard mechanical lock cylinder. They retrofit into the lock hardware with the ease of a mechanical cylinder and do not change how the lock operates.

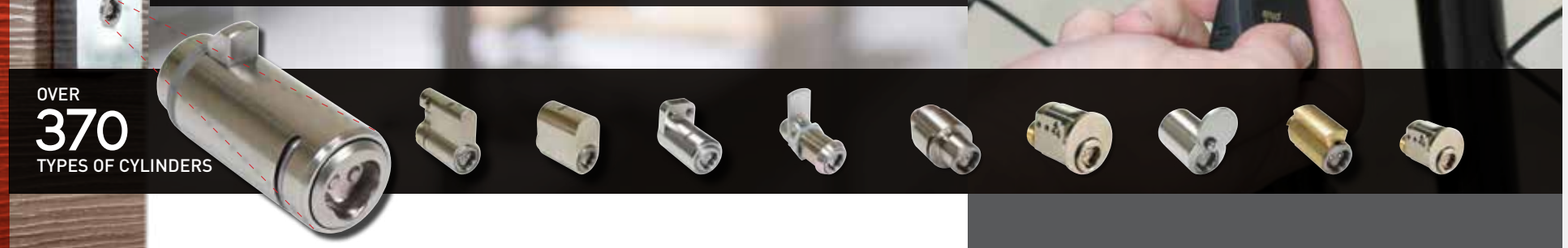
There are over 370 CyberLock cylinders that have been designed for doors, cabinets, padlocks, containers, equipment, safes and more.

Installation is as simple as removing the original cylinder and replacing it with a CyberLock cylinder. Installation requires no wiring or batteries, making installation quick and easy. All power is provided by the CyberKey: when a CyberKey comes in contact with the cylinder, it powers up the CyberLock's circuitry so CyberKey and CyberLock communicate. If the CyberKey is not on the lost CyberKey list and the permissions are correct, the CyberLock will open.

The circuitry stores multiple types of information: encrypted codes that ensure only CyberKeys within the system work with the CyberLock;

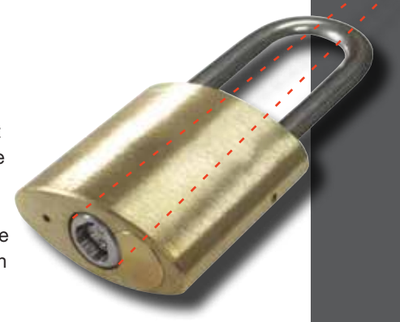
WHY THE CYBERLOCK ELECTRONIC CYLINDER IS SUPERIOR

- Retrofits most mechanical locks
- No wiring and battery required
- Torque brake
- No keyway to pick
- Potted circuits protected against dust, water, salt & air
- Lost key list prevents unauthorised access
- Withstands to 300,000 volts and 18,000 gauss
- Records authorised and denied access



» and a list of lost keys to eliminate access by any CyberKey that is missing or lost.

CyberLock cylinders offer superior physical security. They have no conventional keyway that is vulnerable to being picked. Moreover, if torque is applied to the barrel, the front part separates from the back half. The back half of the barrel expands, causing a brake effect that engages the sides of the cylinder's case, stopping the rotation and leaving the cylinder in the locked position.



SUITABLE FOR OTHER BRAND PADLOCKS

EKA CyberLock has a cylinder (IP68) which is easily retrofitted into other brands of padlocks.

The weather resistant cylinder is sealed to prevent dirt and water from entering into the back of a cylinder.

Applications include storefronts, gates, construction sites, equipment or any padlock location needing access control.

IP68 WATER PROOF · DUST PROOF · NO WIRING · NO BATTERY

EKA CYBERLOCK PADLOCKS

EKA CyberLock IP68 rated Brass Body, Stainless Steel Shackle Padlock.

The EKA CyberLock padlock is a Wilson Bohannan 8900 series padlock with the EKA CyberLock weather resistant cylinder pre-installed.

It has a solid brass body and a stainless steel shackle. The retainer, ball bearings and shackle pin are also stainless steel.

Three shackle lengths are available as indicated by below:

- 26mm shackle
- KR 26mm shackle, key-retaining
- 50mm shackle
- KR 50mm shackle, key-retaining
- 75mm shackle
- KR 75mm shackle, key-retaining

With the key-retaining padlocks, the shackle must be returned to the closed position before the key can be removed.

Snap shut and high security padlocks are also available.

MANAGEMENT SOFTWARE

CYBERAUDIT

Advanced monitoring and reporting.

EKA CyberLocks server based software, CyberAudit Web, is designed to simplify the management of your system. The software is available as a self hosted application or a fully supported and managed cloud based solution.

A hierarchy of administrators allows individual managers responsibility for only the CyberLocks and the people in their area. It even manages assets across countries and time zones.

An intuitive point-and-click browser-based interface that uses drop-down information boxes is all that's needed to access the modules that drive EKA CyberLock's access control, monitoring and reporting capabilities.

iOS amazon web services SELF-HOSTED

KEY AND CUSTOM MODULES

Location Graphics. Create a graphical interface of your system that allows you to place the location of CyberLocks and Communicators for improved tracking and auditing.

Door & Input / Output Support. Through Flex, manage access to Wiegand-compatible third-party systems such as swipe cards, RFID and biometric readers. Doors can also be set to unlock and relock at certain times and alarms can be triggered if a door is forced or left open.

CyberLocks. See all CyberLocks and individually set access and reporting characteristics. Options include: delayed access, access only with a number of CyberKeys and email notification of denied access.

People and CyberKeys. Allocate individual CyberKeys to users. Set days and times they have access to certain CyberLocks, how soon the CyberKey's access permissions expire and even revoke a lost CyberKey.

Schedules. Set schedules of who can go where and at what time. This can be as specific as a few minutes at a certain time on one or two days of each week.

Reports. Audit trails can be used to generate tailored reports that tell you who has been where and when. Anything from specific people to user-defined groups such as: contractors, cleaners, security staff and weekend users.

FEATURES

- Dashboard reporting with management console
- Over 527 different access events allowing administrators to produce hundreds of different types of reports
- Detailed audit trail
- Set two, three or four-way access
- Denied access email alerts
- Hierarchy of administrators
- Remote key initiation via smart devices
- Key scheduling and expiry
- Set delayed access
- Set group access permissions
- Multiple time zone management
- Monitors and controls third-party systems

EKA CYBERLOCK

COMMUNICATION DEVICES

Communicators underpin the flexibility of EKA CyberLock. Simple, instant key activation.

Communicators serve as the interface between CyberLock hardware and the CyberAudit management software. Through a communicator, CyberKey information is downloaded into the software and new schedules and permissions are uploaded on the CyberKeys.

A variety of communicators are available to address individual facility and personnel needs. Communicators can be installed in locations that are easily accessible to your CyberKey holders such as an employee entrance, sign in desk or even a car park access point, making frequent CyberKey expirations and access programming convenient for higher security.

A network of communicators (each communicator can be given an IP address) allows users to validate their CyberKeys without returning to where the EKA CyberLock software is hosted, instantly downloading audit trail data and receiving updated access permissions. Some communicators are also designed to recharge rechargeable CyberKeys.

Communicators are so versatile that they can be mounted almost anywhere, maximising ability to control access to even the most remote assets.

VALIDIKEY 2 VAULT

This vault can hold and program up to two CyberKey smart keys. It has a door that locks to secure the keys until an approved RFID card is scanned or a mission number is entered on its display keypad. After verifying the mission from its internal cache, the ValidiKey 2 programs a key with that user's permissions, unlocks the door and prompts the user to remove the key.

MINI KEYPORT

This smaller version of the authoriser keypad can be employed when the additional security of keypad and PIN codes are not required.

Simple, instant key activation.

20-KEY VAULT CABINET

Ideal for large facilities, this intelligent key cabinet stores keys in an inactive state.

An RFID card or PIN code is required to activate a CyberKey and when a CyberKey is returned to the vault, it automatically deactivates with a full audit of the CyberKey activities downloaded to the CyberAudit.

AUTHORISER KEYPAD

An authoriser keypad is a durable, weather-proof unit that is fitted to the exterior of a building or facility.

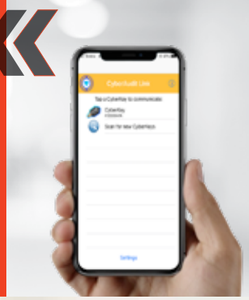
Users present their key to the authoriser and enter a PIN code to obtain permission privileges.

USB STATION

In a smaller office, when your CyberAudit might only sit on a desktop, a simple USB station port is a cost-effective way to authorise keys.

CYBERAUDIT LINK APP

The smart device app enables each user to activate & deactivate a CyberKey Blue 2 in-situ, as well as communicate with CyberAudit, allowing real time audit reporting and update of permissions.



Communicator Facts

- Every update simultaneously downloads key activity and updates key permissions.
- Several communicators offer multiple functions, such as charging the key battery or storing unprogrammed keys.
- Communicators available depends on the key type.
- Several communicators are available to address individual, facility and personnel needs.

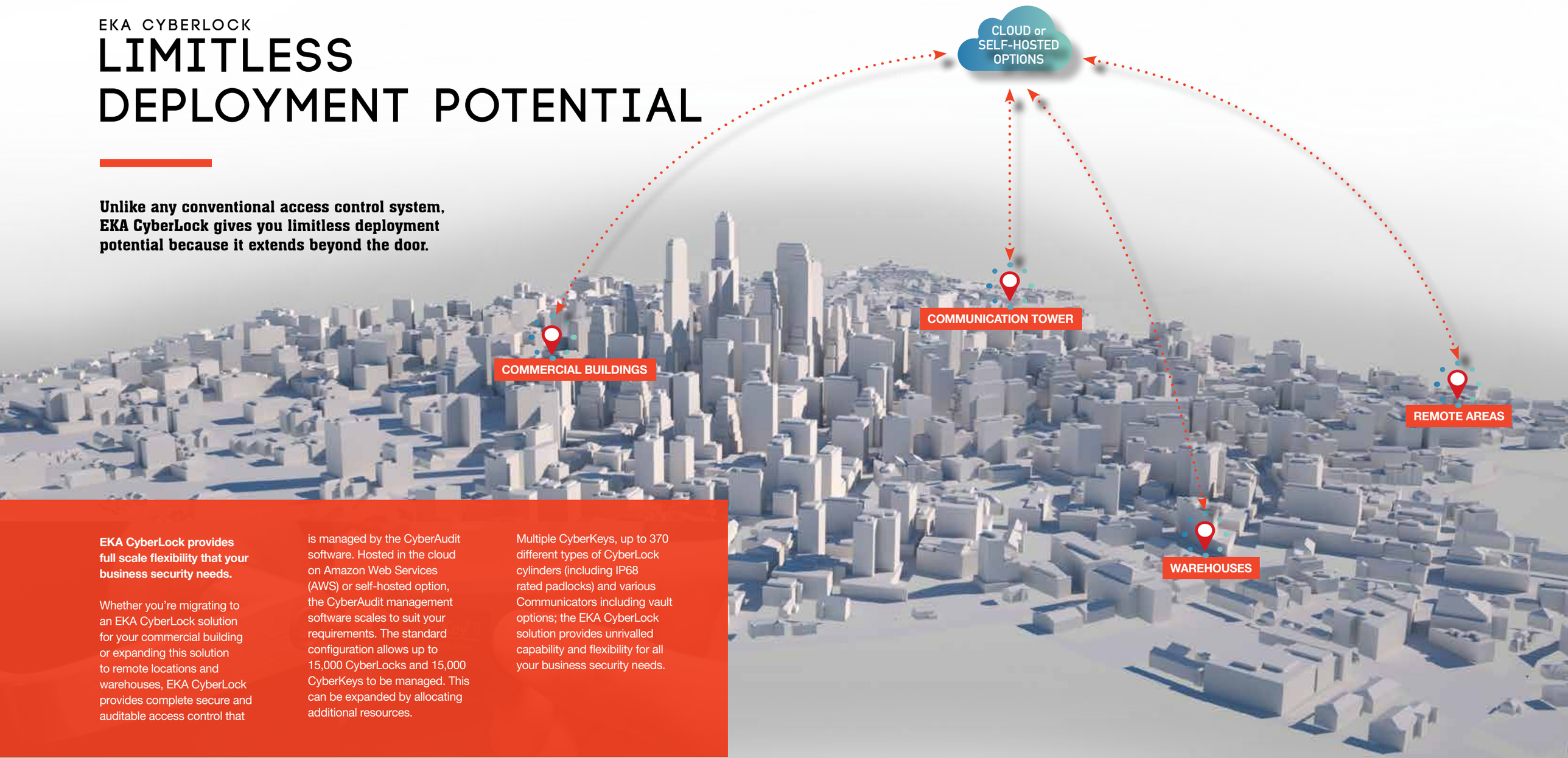
CYBERKEY VAULT

The CyberKey Vault houses a single CyberKey. The unit is an extremely secure, rugged, outdoor vault that stores an un-programmed CyberKey. When approved credentials are presented, the CyberKey is programmed and can then be removed from the vault.

EKA CYBERLOCK

LIMITLESS DEPLOYMENT POTENTIAL

Unlike any conventional access control system, EKA CyberLock gives you limitless deployment potential because it extends beyond the door.



EKA CyberLock provides full scale flexibility that your business security needs.

Whether you're migrating to an EKA CyberLock solution for your commercial building or expanding this solution to remote locations and warehouses, EKA CyberLock provides complete secure and auditable access control that is managed by the CyberAudit software. Hosted in the cloud on Amazon Web Services (AWS) or self-hosted option, the CyberAudit management software scales to suit your requirements. The standard configuration allows up to 15,000 CyberLocks and 15,000 CyberKeys to be managed. This can be expanded by allocating additional resources.

Multiple CyberKeys, up to 370 different types of CyberLock cylinders (including IP68 rated padlocks) and various Communicators including vault options; the EKA CyberLock solution provides unrivalled capability and flexibility for all your business security needs.

MANY LOCKS;

ONE CONTROL INTERFACE

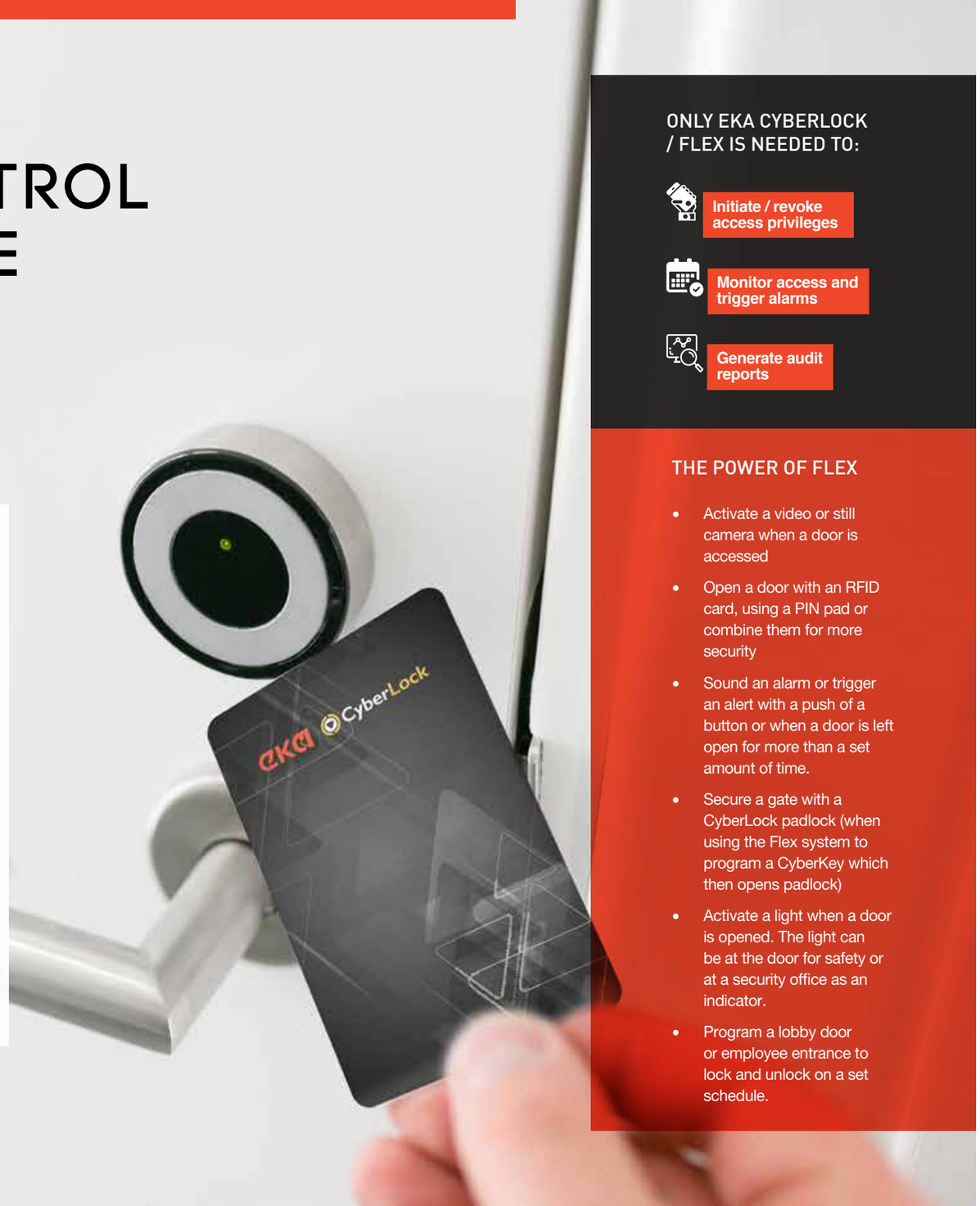
One system for many locks: indoors, outdoors, mobile and remote.

Until now, if you installed different types of locking systems you had no choice except to operate and manage them independently.

Sitting side-by-side, the result is more expense, more operational work for facility and asset managers, and more opportunities for security breaches.

EKA CyberLock solves this through a system that can deliver single, unified access control.

Through a hub called Flex, EKA CyberLock is able to integrate with and manage virtually any other access control device that uses a Weigand compatible input device-from RFID, to electronic swipe and HID, Maglocks, electronic strikes, and even bio-metric devices, all managed under one unified software platform.



ONLY EKA CYBERLOCK / FLEX IS NEEDED TO:

- Initiate / revoke access privileges
- Monitor access and trigger alarms
- Generate audit reports

THE POWER OF FLEX

- Activate a video or still camera when a door is accessed
- Open a door with an RFID card, using a PIN pad or combine them for more security
- Sound an alarm or trigger an alert with a push of a button or when a door is left open for more than a set amount of time.
- Secure a gate with a CyberLock padlock (when using the Flex system to program a CyberKey which then opens padlock)
- Activate a light when a door is opened. The light can be at the door for safety or at a security office as an indicator.
- Program a lobby door or employee entrance to lock and unlock on a set schedule.

ONE SYSTEM

The CyberLock Flex System is an access control solution that offers both hard-wired and key-centric technologies managed within one software package.

TWO TECHNOLOGIES

Use Flex modules to increase security at high traffic doors and incorporate additional security features such as cameras and alarms. Use CyberLock cylinders and padlocks–which don't require wiring to secure other low use conventional doors and even remote locations.

THE PERFECT UNION

There is no longer a need to choose between the versatility of a key-centric system and traditional, hard-wired access control. With the CyberLock Flex System, you have the best of both worlds.

COMPATIBLE

The Flex System is managed by CyberAudit management software, the same platform behind the award-winning CyberLock access control system composed of electronic lock cylinders and programmable smart keys.

FLEXIBLE

The heart of the system is built around the Flex System Hub access controller which provides connections for and power to weatherised modules that can be mixed and matched to fit your access control needs.

EXPANDABLE

A wide variety of other security devices such as HID readers, request-to-exit devices, alarms, door sensors and more can be added to the Flex System through the Door Controller & I/O module.

INFINITE POSSIBILITIES

Protect assets by securing office doors, cabinets, gates and more.

CACHE MEMORY

An internal access profile cache allows the Flex Hub to continue to function even during a network outage. Built in external battery management means power failure does not compromise performance.

EKA CYBERLOCK IS THE

COMPLETE ACCESS CONTROL SYSTEM

Whether it's a cage, cupboard, case, container, cash bag or gate, if you can put a lock on it, EKA CyberLock can secure and control it.

HOW EKA CYBERLOCK COMPARES TO OTHER REMOTE ACCESS SYSTEMS

FEATURE	MECHANICAL KEY	ACCESS CONTROL	EKA CYBERLOCK
Low upfront cost	●		●
Expand as you grow	●		●
Secure beyond the door	●		●
Low impact install	●		●
No power issues	●		●
No keyway		●	●
Highly resistant key duplication		●	●
Set access permissions		●	●
Audit trails		●	●
Secure remote facilities	●		●
One software platform			●
Secure mobile assets	●		●

8 UNIQUE REASONS WHY EKA CYBERLOCK IS THE COMPLETE ACCESS CONTROL SYSTEM

1 ONE SOFTWARE PLATFORM.

EKA CyberLock bridges existing hardwired and key-centric security solutions and can secure, control and audit access to both types.

2 WORKS BEYOND THE DOOR.

Whether it's a cage, cupboard, case, container, cash bag or gate, if you can put a lock on it, EKA CyberLock can secure and control it.

3 STAYS UP WHEN THE POWER IS DOWN.

If the power goes down a hardwired access control systems may fail. EKA CyberLock are powered-up as required by the CyberKey your people carry for access.

4 NO EXPENSIVE AND DISRUPTIVE CABLING.

Unlike traditional access control systems that need extensive hardwiring, the EKA CyberLock cylinder retrofits into existing door hardware without the need to hardwire.

5 MORE COST EFFECTIVE.

EKA CyberLock delivers every advantage of an access control system at a cost per door (lock) that's comparable with a master key system.

6 AUDIT ACCESS TO ANY ASSET.

You can access audit trails even for mobile and remote assets and see exactly who's been in and out, as well as who has tried and been denied.

7 DEPLOYS TWICE AS FAST.

Current access control technology is slow to install and deploy. Even in large organisations with thousands of assets to secure, EKA CyberLock can be fully installed and running in just a couple of weeks.

8 A SINGLE KEY OPENS ANY LOCK.

As long as they have access privileges, your people can access any asset using just one key.

THE PREFERRED ACCESS CONTROL

FOR ANY INDUSTRY OR SECTOR

EKA CyberLock's next-gen access control technology is the cutting edge security solution for any industry or sector that needs a sure way to secure, control and audit assets that extend beyond the door.

Telcos and data centres.
EKA CyberLock can be used to secure access to communication pits, racks and cages.

Utilities.
Large utilities like water boards can secure facilities like power plants, sub-stations, equipment and storage.

Government.
Assets ranging from offices and halls, to depots, parking meters, barriers and park toilets can all be easily secured with EKA CyberLock.

Transport and logistics.
Containers, yards, warehouses, depots and even gates can be secured using EKA CyberLock.

Airports.
EKA CyberLock will secure access to hangers, gates, utility and server rooms and restricted access areas.

Remote Sites.
Covering thousands of locks across vast geographical distances such as traffic light systems, communication towers, power systems and more.

Mining and construction.
Stop wondering who has access to plant equipment, vehicles and explosives. EKA CyberLock secures and tracks it all for you.

Education and office.
EKA CyberLock can be used to secure access to utility doors with padlocks, cash tins, access panels, air conditioning, display units, light boxes and even roller doors.

EKA CYBERLOCK IN ACTION

Migrating to an EKA CyberLock access control system is simple. With virtually no impact to your day to day business as installation time is only a few minutes per lock, which is only a fraction of a traditional cabled system. What's more, the process is simple, efficient and transparent. Here's how it works.

STEP 01

IDENTIFY
The assets you need secured and survey the sites to identify the CyberLock cylinders you require.

STEP 02

ASSIGN
Using the CyberAudit management software create user specific access profiles and allocate CyberKeys.

STEP 03

INSTALL
The CyberLock cylinders, padlocks, camlocks and more. Installation time is normally only a few minutes per door.

STEP 04

DISCARD
Old mechanical keys. Staff members, contractors, security providers and others requiring keys now only need a single CyberKey.

STEP 05

MONITOR AND REPORT
The CyberAudit software can be used to create access profiles and audit reports, block lost keys, add additional users and customise and refine access profiles as required.

STEP 06

EXPAND
Your EKA CyberLock system can easily be expanded. New locks can be added to your system be they for a door, a padlock or a cabinet. Moreover, the expansion is not limited by geography with the system easily expanded to different sites, from the lock around the corner, in another state or the other side of the world.