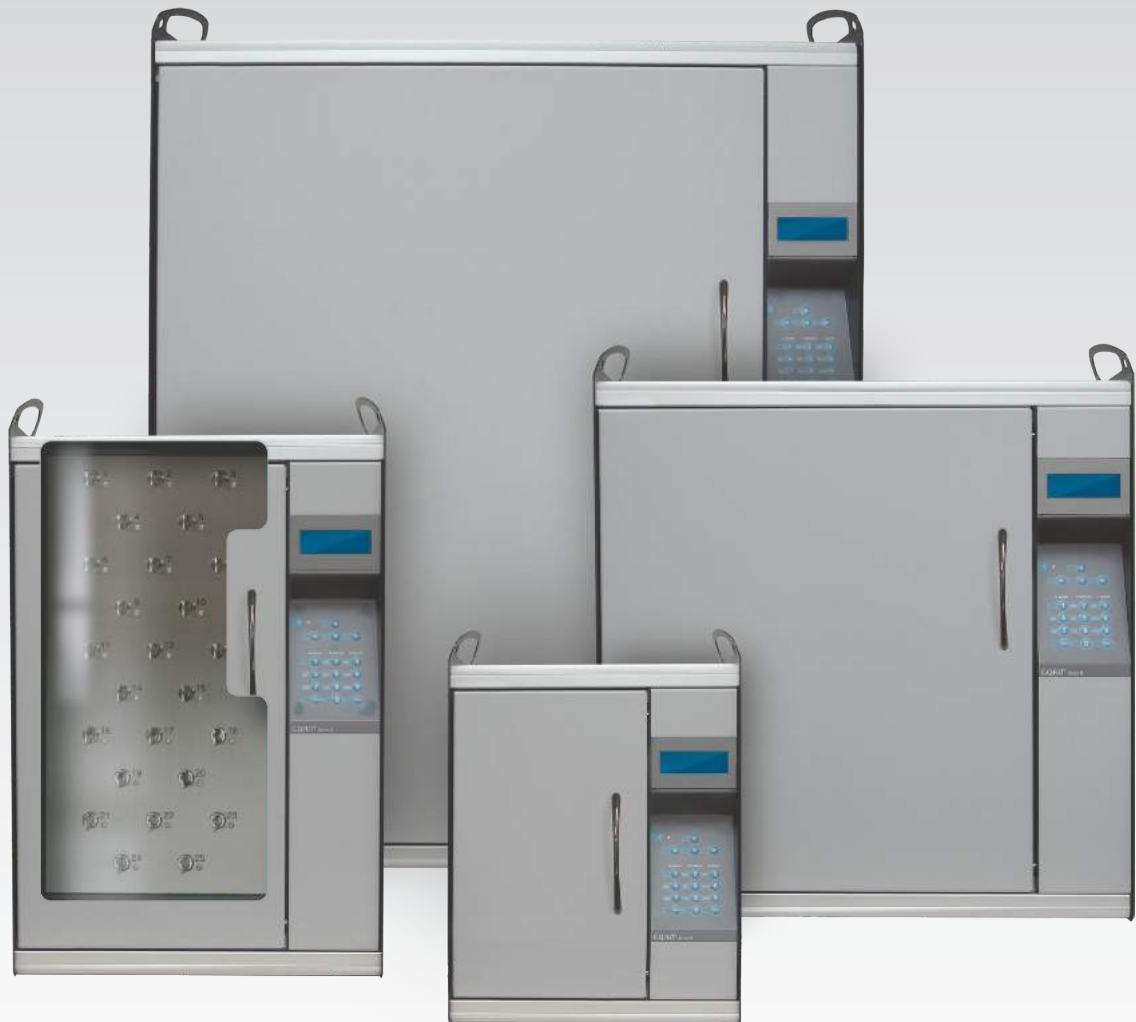


C.Q.R.iT[®]

electronic key cabinets



Smart solutions for
managing keys



CIC TECHNOLOGY

C.Q.R.iT[®] Key Cabinets

C.Q.R.iT[®] key cabinets are the ultimate in security and convenience. Completely automate the process of signing keys in and out. Decide exactly who gets access to what, when and for how long.



AUTHORISATION

The door is secured with a two-point locking system that can only be opened by authorised users.

CONTROL

Each set of keys is individually controlled, allowing you to restrict access based on user, group, time or quantity.

ACCESS

Once the door is unlocked, users can only access the sets of keys they're allowed – all others remain locked in place.

ALARMS

Alarms will always be logged and recorded in the software. They can also be audible at the cabinet, they can send an email and/or relay the signal to an existing alarm panel.

UNIFIED SOLUTION

These cabinets manage your existing keys regardless of type and profile. They can also integrate with your existing readers, access control systems or alarm panels.

REPORTING

Every action or violation at the cabinet is automatically recorded giving you real-time evidence of all transactions and instant access to accurate reports.

PIN

PROX CARD

FINGERPRINT

OTHER
e.g. facial recognition



TRANSACTION RECORDED

Asset: Vehicle #3
Action: Key taken
User: John Smith
Date: 11/10/18 10:34am

5pm

KEY NOT
RETURNED

AUTHENTICATION

KEYS RELEASED

ACCOUNTIBILITY

ALARMS

KeySecure® Software

The KeySecure® software is flexible and intuitive. It makes light work of even the most complex access control and monitoring tasks.



ALARMS

Customisable alarms include: door forced, tamper detection, AC power out, key timer expired.



MAX KEYS OUT

Limit the number of items each user is allowed out of the cabinet at any one time.



EMAIL ALERTS

Configure automatic emails to give you real-time information of any violations, even if you're offsite.



TIME ZONES

Restrict the times that users may access certain keys. E.g., Monday to Friday, 9am - 5pm.



TIMER

Place timers on certain items and receive notifications if they haven't been returned within that period.



ENCRYPTED COMMUNICATION

256-bit AES encryption is used to communicate between the central database and the cabinets.



SAME USER RETURN

Ensure that the user who removed a key is the same one to return it, increasing the accuracy of audit trails.



FLEXIBLE ALLOCATION

Single key positions (bunches) or groups can be allocated to individuals or groups of users.



MULTI CUSTODY

For sensitive items, demand that more than one authorised user is present to sign it out.



NETWORK + USB

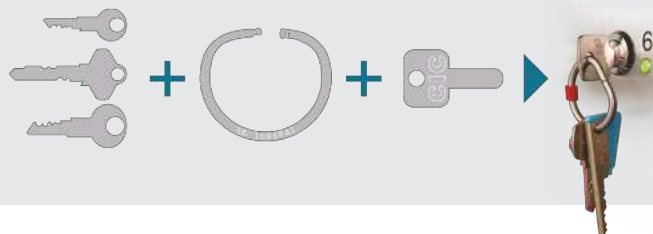
Fully integrated network capabilities (TCP/IP) as well as a USB port inside the door for full upload / download.

TAMPER-PROOF KEY RINGS®

These high security rings seal permanently into a continuous loop making it impossible to substitute keys without detection. Each key ring is engraved with a unique serial number for maximum accountability.

DIAMETER CAPACITY (approx)

3cm	1-5 keys
4cm	5-10 keys
5cm	10-15 keys
7cm	15-25 keys
9cm	25-50 keys



FULLY INTEGRATED SOLUTION



For ultimate convenience, C.Q.R.iT® cabinets can be controlled through a third party system, reducing data entry, improving accuracy and simplifying reporting. In some cases you will even be able to prevent users from exiting the building without returning their keys.

SIZES



C.Q.R.iT 12

Capacity: 12 bunches
Height: 540mm
Width: 665mm
Depth: 170mm
Weight: 12.5kg



C.Q.R.iT 25

Capacity: 25 bunches
Height: 760mm
Width: 705mm
Depth: 170mm
Weight: 25kg



C.Q.R.iT 50

Capacity: 50 bunches
Height: 760mm
Width: 920mm
Depth: 170mm
Weight: 32kg



C.Q.R.iT 100

Capacity: 100 bunches
Height: 1050mm
Width: 1090mm
Depth: 170mm
Weight: 60kg

Please note: the above dimensions represent the total space required on the wall, including access for maintenance and installation. Actual cabinet is smaller and fits within this footprint. Weight refers to empty cabinet.

ACCESSORIES



PROX READERS

C.Q.R.iT® cabinets can integrate with almost any prox reader so users can authenticate by presenting a card.



BREATHALYSERS

Make sure your users are under the legal limit before they can access vehicle or plant keys.



COLOURED KEY TAGS

For easy visual identification, keys can be colour-coded without adding unnecessary bulk to your bunches.



TAMPER PROOF CARD HOLDERS

These allow you secure and manage prox cards by attaching to the holder keys within the cabinet.



FINGERPRINT SCANNERS

To protect against PIN or card sharing, fingerprint scanners can be used to identify users.



FACIAL RECOGNITION

Authentication at the cabinet can also occur with increasingly popular facial recognition technology.



DYNAMITE BUTTON

For use in emergencies, administrators can use this button to release all keys.



KEY SHIELD

This hides the cut of important keys when hanging in the cabinet so they can't be copied.

Telephone: 1300 723 796

Email: sales@safeguardlocksmiths.com.au

Website: www.safeguardlocksmiths.com.au

