KL1100

SLEEK AND SUBTLE

KL1100 is the latest addition to the KitLock by Codelocks range of locker locks.

LOCK MANAGEMENT
Program individual or multiple locks remotely using the Codelocks Cloud Portal. Alternatively program locally using our plug-in programmer.

STYLISH DESIGN
The slimline front plate and integrated handle adds a touch of style giving any locker or environment a contemporary feel.

EASY OPERATION
Behind the stylish design sits an electronic latch containing the technology and power for maximum functionality.

FUNCTIONS

Private Function
This is the default function and is already pre-programmed in new locks. This function is used where the same card client will be repeatedly used, e.g. an employee/pupil with a personal locker.

Public Function
Suitable for short term use by different users. This mode can support up to 50 card clients. Suitable for use in short term multi-occupancy applications such as leisure centres, spas and hotels.

TECHNICAL SPECIFICATION

Management	**Local** Using our plug-in programmer, set-up and configure the KL1100 - register up to 50 Card Clients per lock **Remote** Using the Codelocks Cloud Portal program individual or multiple locks using an initialisation card Card Clients can be managed and assigned to multiple locks and lock groups (max. 20 per client).
Low Battery Warning	Red LED will flash on opening to indicate low battery
Power	Powered by 4 x AA batteries (supplied)
Battery Override	Connect to 5V micro USB power source for temporary power
Door Thickness	Ready to fit doors up to 25mm (1”)
Memory	Non-volatile memory will be retained
Latch	Electronic latch
Card Client Types	Master, Technician and User - supports MIFARE® Classic 1k
Installation	Vertical; Horizontal (additional components required)
Material	Mixed plastic and alloy construction

PROGRAMMING

Group	Title	Description
General	Initial set-up	On power-up, blue & red LEDs will flash simultaneously, and the lock will be in an unlocked state.
	Initialise for private use	1. Touch a MIFARE card to the lock (this becomes the Master User Card) 2. A double LED flash will confirm acceptance 3. Wait 5 seconds - lock will enter private use
	Initialise for public use	1. Touch a MIFARE card to the lock 2. A double LED flash will confirm acceptance 3. Touch a second MIFARE card to the lock within 5 seconds - this card becomes the Technician User Card 4. By repeating stage 3 up to 10 times will allow you to add up to 10 Technician User Cards 5. Once complete, wait 5 seconds and the lock will enter public use

	Change operation function	Perform factory reset
		
		or with the optional Codelocks Keypad Accessory Unit:
		
		1. Plug the Codelocks Keypad Accessory Unit into the lock
		2. Touch Master User Card to lock
		3. On the keypad, enter:
		  1. Public Use: press # • 24 • 24 ••
		  2. Private Use: press # • 26 • 26 ••

	Add/Remove Technician Cards (Local)	**Note:** The Codelocks Keypad Accessory Unit is required for this function
		
		1. Plug the Codelocks Keypad Accessory Unit into the lock
		2. Touch Master User Card to lock
		3. Press # • 04 •• on the keypad
		4. Within 5 seconds, touch Technician User Card to lock
		    1. If the Technician User Card already exists, it will be removed
		    2. If the Technician User Card does not exist, it will be added (maximum of 10)
		5. Once complete, wait 5 seconds and the lock will return to public use
		
		Note: Presenting the Master User Card to the lock will open the lock and remove any User Cards

	Change Master Card	Perform factory reset or with the optional Codelocks Keypad Accessory Unit: 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch Master User Card to lock 3. On the keypad, enter: 1. Press # • 01 • 01 •• 4. Touch new Master User Card to lock
	Remove all Technician Cards (Local)	Perform factory reset or with the optional Codelocks Keypad Accessory Unit: 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch Master User Card to lock 3. On the keypad, enter: 1. Press # • 05 • 05 ••
	Re-lock Delay	**Note:** The Codelocks Keypad Accessory Unit is required for this function 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch the **Master User Card** to the lock 3. On the keypad, enter: 1. Press # • 06 • Time <02-30> ••

	LED Locked Indicator	Enabled by default.
		
		To disable, you will require the Remote Card Authorisation **or** the optional Codelocks Keypad Accessory Unit are required:
		
		1. Plug the Codelocks Keypad Accessory Unit into the lock
		2. Touch Master User Card to lock
		3. On the keypad, enter:
		    1. Press # • 08 • 01 •• to disable (default)
		    2. Press # • 08 • 02 •• to enable

	Enable Public Pairing	Public pairing is enabled by default and cannot be disabled
	Factory reset	TO DO To be confirmed by Kingtronics

	Setting up time-based functions	**Note:** The Codelocks Keypad Accessory Unit is required for this function
		
		The lock has the following time-based functions:
		
		• Open after x hours
		• Open at xx:yy time *
		
		* Requires date/time to be set
		
		1. Plug the Codelocks Keypad Accessory Unit into the lock
		2. Touch the **Master User Card** to the lock
		3. Enter the current date/time in the format:
		    ○ Press # • 12 • yyMMddhhmm • <1-7> ••
		    ○ E.g: For Friday 28th September 2018, 12:15, enter: # • 12 • 1808281215 • 5 ••
		    ○ The <1-7> will correspond with the day of the week start with Monday as 1, Tuesday as 2 etc.

	Open after x hours	**Note:** The Codelocks Keypad Accessory Unit is required for this function 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch the **Master User Card** to the lock 3. On the keypad, enter: 1. Press # • 10 • <Hours to remain locked> ••

	Open at set time	**Note:** The Codelocks Keypad Accessory Unit is required for this function **Note:** Date/time must be set for this function 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch the **Master User Card** to the lock 3. On the keypad, enter: 1. Press # • 11 • <Hour at which to unlock - hh format> ••
	Dual authorisation	**Note:** Where any two Card Clients are required to open the lock (either a standalone, User Card (local), or a Remotely Authorised Card. 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch the **Master User Card** to the lock 3. On the keypad, enter: 1. Press # • 12 • <0 to disable|1 to enable> ••

User Management	Add/Remove User Card (Local) (Private Use)	1. Touch the Master User Card to the front of the lock
		2. Touch a User Card to the front of the lock
		    1. If the User Card is not already registered, it will be added
		    2. If the User Card is already registered, it will be removed
		3. Repeat step 2 within 5 seconds to continue adding/removing User Cards
		4. Once complete, wait 5 seconds and the lock will return to normal operation
		
		Note: Presenting the Master User Card to the lock will cause the lock to unlock.

	Removing all User Cards (Local) (Private Use)	Perform factory reset or with the optional Codelocks Keypad Accessory Unit: 1. Plug the Codelocks Keypad Accessory Unit into the lock 2. Touch Master User Card to lock 3. On the keypad, enter: 1. Public Use: press # • 08 • 08 ••

General	Low battery	When the battery power is low the Red LED will flash three times before the Blue LED flashes to signal acceptance of the smart card. Batteries should be changed as soon as this happens. The lock will operate for approximately 100 times with low battery. On a no-power event, power may be supplied via the USB connector on the front-plate. Use the Master User Card to open the lock and change the batteries.

Remote Card Authorisation	Codelocks Card Manager Client installation	To use RCA, you must meet the following prerequisites:
		
		• Have a Codelocks Portal account (free to sign-up)
		• Have purchased the Codelocks Keypad Accessory Unit
		
		Set-up:
		
		1. Sign into Portal - navigate to Remote Card Authorisation > Register & Install Card Manager Client
		2. Enter a name for the particular Card Manager Client. E.g. if the software and USB card reader are being installed in reception, you could enter "Reception"
		3. Click "Save"
		4. Once the information has been saved, follow the on-screen instructions. **Do not leave the page or close your browser window until you have followed the installation instructions**:
		    1. Download and install the Codelocks Card Manager Client software
		    2. During installation, you will be asked for the security certificate - copy this from the on-screen instructions and paste it into the box provided
		5. Once installation is complete, a confirmation message will be displayed

	Create lock group	Create Lock Group Initialisation card via Portal & desktop software. This card will enable RCA on the respective locks.
		
		1. Sign into Portal - navigate to Remote Card Authorisation > Create Lock Group
		2. Select lock model (KL1100)
		3. Enter a name and location for your Lock Group
		4. Select the timezone for the Lock Group
		5. Enter the starting Lock ID - this must be an integer value. The first lock to be initialised will be assigned this ID. After the first lock to be initialised, the next lock will be initialised with an incremented ID and so on.
		6. Enter the number of locks that you will initialise
		    1. **Note:** This value must be accurate otherwise you will may not be able to correctly add locks to cards
		7. Click Save & Commit
		8. Open your Codelocks Card Manager Client software (on your PC), place a MIFARE card on the USB card reader
		9. From the list of available actions, select the "Lock Group Initialisation" action
		10. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed and you will be able to use the card to enable RCA on the respective locks.
		    1. **Note:** This Initialisation Card must be kept secure and/or destroyed after use. This card is NOT the same as a Master Card.
		
		TO INITIALISE THE LOCKS, REFER TO ***Lock Initialisation***.

	Add additional locks to an existing group	Additional locks can be added to existing Lock Groups:
		
		1. Sign into Portal - navigate to Remote Card Authorisation > Lock Groups
		2. Select the Lock Group that you would like to add new locks
		3. If you chose to not have the Portal remember the Lock Group ID, enter the Lock Group ID manually
		4. Enter the starting Lock ID - this must be an integer value. The first lock to be initialised will be assigned this ID. After the first lock to be initialised, the next lock will be initialised with an incremented ID and so on.
		    1. **Note:** Check that you use a consecutive ID from the end of the existing group
		5. Enter the number of locks that you will initialise
		    1. **Note:** This value must be accurate otherwise you will may not be able to correctly add locks to cards
		6. Click Save & Commit
		7. Open your Codelocks Card Manager Client software (on your PC), place a MIFARE card on the USB card reader
		8. From the list of available actions, select the "Add Locks to Lock Group" action
		9. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed and you will be able to use the card to enable RCA on the respective locks.
		    1. **Note:** This Initialisation Card must be kept secure and/or destroyed after use. This card is NOT the same as a Master Card.
		
		TO INITIALISE THE LOCKS, REFER TO ***Lock Initialisation***.

	Replace a lock within a group	1. Sign into Portal - navigate to Remote Card Authorisation > Lock Groups
		2. Select the Lock Group
		3. If you chose to not have the Portal remember the Lock Group ID, enter the Lock Group ID manually
		4. Select the lock you wish to replace/deactivate
		    1. Replace: Click "Replace or Re-initialise Lock"
		    2. Deactivate: Click "Deactivate"
		        1. **Note:** This option deactivates the lock within the Portal. You may still need to remove the physical lock
		5. Click Save & Commit. If you are replacing or re-initialising a lock, continue. Otherwise, there are no further steps.
		6. Open your Codelocks Card Manager Client software (on your PC), place a MIFARE card on the USB card reader
		7. From the list of available actions, select the "Re-initialise Lock" action
		8. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed and you will be able to use the card to re-initialise the respective lock.
		    1. **Note:** This Initialisation Card must be kept secure and/or destroyed after use. This card is NOT the same as a Master Card.
		
		TO INITIALISE THE LOCK, REFER TO ***Lock Initialisation***.

	Card authorisation	1. Sign into Portal - navigate to Remote Card Authorisation > Authorise Card
		2. Select card type (User, Technician or Master)
		    1. **User:** Can be permitted access to any lock or lock group selected
		    2. **Technician:** Can permitted access to any lock or lock group selected. After use on a locked Public Mode lock, lock will return to a locked state.
		    3. **Master:** Can be permitted access to any lock or lock group selected. Can also be used to transfer new settings to a lock.
		3. Select the locks or lock groups that you want to authorise access to
		4. Select card expiry date
		5. Select access pattern
		    1. Days of the week (MO to SU)
		        1. Hours of the day on each of the days (00 to 23:59)
		6. If you chose to not have the Portal remember the Lock Group IDs, enter the Lock Group IDs manually against each Lock Group
		7. Click Save & Commit
		8. Open your Codelocks Card Manager Client software (on your PC), place a MIFARE card on the USB card reader
		9. From the list of available actions, select the "Authorise Card" action
		10. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed.
		    1. The CCMC software will include the UID of the new card in the Status Update Response

	Lock Initialisation	1. Touch the **Initialisation Card** to the lock
		    1. **Note:** An Initialisation Card cannot be used on a lock that has already been initialised. The lock must be factory reset before it can be re-initialised.
		    2. **Note:** Initialisation sets all lock details including the lock ID
		2. A double flash indicates success

	Update lock settings	Via Remote Card Authorisation, it is possible to update some lock settings by using the Master Card to transfer new commands to the lock. Settings that can be altered include: • Set Private Use • Set Public Use • Set Dual Card Authorisation (Private Use Only) • Set Locked Indication • Set Unlock at X Time • Set Unlock after X Hours Process for transferring commands to a lock: 1. Sign into Portal - navigate to Remote Card Authorisation > Lock Groups 2. Select the Lock Group 3. Select the command(s) that you wish to amend and configure any required parameters 4. Click Save & Commit 5. Open your Codelocks Card Manager Client software (on your PC), place the Master User Card on the USB card reader 6. From the list of available actions, select the "Set Commands" action 7. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed 8. Touch the Master Card to each lock in turn - settings will automatically be applied to the lock.

	Blocking a Card	Via Remote Card Authorisation, a **User** or **Technician Card** can be blocked. A card can only be blocked if the card UID is known. 1. Sign into Portal - navigate to Remote Card Authorisation > Clients 2. Select the Client (User/Technician Card) that you want to block. Note that multiple clients can be selected. 3. Select the **Block Action** and Click Save & Commit 4. Open your Codelocks Card Manager Client software (on your PC), place a Card on the USB card reader - this will become a "Block Card". Note that any data on this card will be overwritten so for example, do not use your Master Card. 5. From the list of available actions, select the "Set Commands" action 6. In the CCMC software, click "Apply" - once the information has been written to the card, a confirmation message will be displayed 7. Touch the Block Card to each lock on which you want to block the cards in turn - settings will automatically be applied to the lock.

CARD BEHAVIOUR

Use	Card Type	Latch Default State	Opens Lock	Can Lock	Deletes Current User Card
Public	Master	Open	Yes	No	Yes
Public	Technician	Open	Yes	N/A - lock re-locks automatically	No
Public	User	Open	Yes	Yes	Yes
Private	Master	Closed	Yes	N/A - lock re-locks automatically	With relevant program/action as per POI
Private	Technician	Closed	Yes	N/A - lock re-locks automatically	No

Private	User	Closed	Yes	N/A - lock re-locks automatically	No
All	Block	No Change	No	N/A	N/A

MODE BEHAVIOUR

Mode	Behaviour
Private	Locked by default
Public	Unlocked, latch retracted by default
Public	Locked whilst in-use

FCC

FCC ID: FA5KL1100

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.