USER MANUAL

ACCESS CONTROL SYSTEM
SIMPLY PAD
STYLOS LINE SERIES

ISEO Zero1
ELECTRONIC SOLUTIONS

How to use this manual

Thanks for choosing this innovative ISEO product.

STYLOS LINE Access Control Devices are components of the SIMPLY system, designed for an effective, user-friendly and at the same time, powerful and flexible access control.

This user manual was compiled to offer a guide on the functions, configurations and characteristics of the device.

For the installation of the SIMPLY system, set-up of the opening and other operations not described herein, refer to the installation and configuration manuals, available in the download area of ISEO Serrature's website, at: http://www.iseoserrature.com.

The installation, initial set-up and changes to the setting require the intervention of qualified staff, adequately trained by ISEO.

- Read this manual prior to use the device in order to ensure a safe and proper use
- Preserve this manual as future reference
- Fill out properly and keep updated the Keyplans in order to facilitate future management and changes.

Information icons

Please familiarise with the icons below, for an easy reading of the manual:

WARNING: it indicates situations that could cause harm to people or animals

BE CAREFUL: It indicates situations that could cause damages to the device or other equipment

NOTE: it indicates notes, suggestions and additional information

Information on copyright

Summary

Introduction

SIMPLY is an effective access control system, user-friendly and at the same time, powerful and of high quality.

The SIMPLY system can consists of more Access Control Devices (ACD.).

Any combination is possible between the following ISEO's ACD:

- Credential codes readers and actuators of the STYLOS LINE series
- ARIES Electronic trim
- LIBRA Double knob electronic cylinder

PAD ACD | **STANDARD ACD** | **ARIES** | **LIBRA**

In particular, there are two types of ACD described in this manual, with similar functions but different configurations, based on the different building technology.

The PAD ACD is an credential reader of the STYLOS LINE series, complete with keyboard and display, thanks to which it is possible to browse the menus to configure your door, manage the credentials, the type and special configurations.

The STANDARD ACD is an credential reader of the STYLOS LINE series without input devices, an ARIES electronic trim or a LIBRA double knob cylinder, which management takes place through the presentation of the SPECIAL credential in sequence, or particular cards conceived for this purpose.

The presence of at least a PAD ACD device is required in an installation configured with the Simply PAD system.

In this manual, the LIGHT signals are represented in relation to STYLOS STANDARD ACD device, but the same are also applicable for the ARIES electronic trim and the LIBRA double knob cylinder.

Categories of credentials

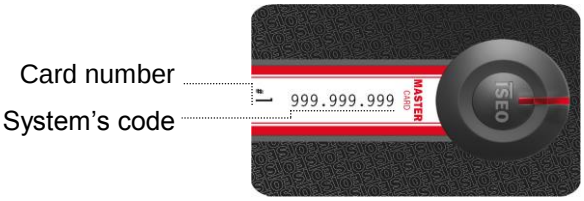
The credentials used in the system can be functionally divided in:

	**MASTER Card** used to “configure” and “manage” the access control system
	**USER Card** used by the users to “open” doors
	**SPECIAL Cards (SET UP, SERVICE, TOGGLE, VIP)** used to enable special doors’ functions

Set of MASTER Credentials for the SIMPLY PAD system

The SET of MASTER credentials consists of 3 cards numbered from 1 to 3.

Each SET of MASTER credentials boasts a univocal system’s code. During the initialization phase with MASTER cards, the system’s code and the relative SET of MASTER cards is associated to the devices.



An improper method and sequence of use of the MASTER credentials could damage the system; therefore, we recommend to strictly follow the instructions relative to the initialization, adding of the cards and updating operations of the SET.

System's operations

The main three operations to carry out on a SIMPLY system are:

1. System's set-up
   - initialization of the access control devices
   - set-up of the parameters of the access control devices
   - compiling of the Keyplan – adding credentials to the White List
2. Delivery of the Credentials to the users
3. Management of the system's updates
   - management of the Keyplan
     - changes to the access criteria
     - management of lost or stolen credentials
   - management of MASTER credentials
     - management of lost or stolen MASTER credentials

All these operations can be performed exclusively by staff holding an enabled MASTER CARD.

Initialization of the access control devices

The new SIMPLY device is in "*Factory Mode*" configuration, meaning with the list of authorised users (White List) empty and no system's code assigned.

The system's initialization takes place through the programming of the ''system's code'', using MASTER Card **#1.**

BE CAREFUL: for the system's initialization, use exclusively MASTER CARD **#1** and put cards #2 and #3 in a safe place. The use of MASTER cards #2 and #3 will be required only if MASTER Card #1 is lost or damaged.

IMPORTANT: all the system's devices must be initialized or updated with the same MASTER Card.

WARNING: in non-initialized ARIES handle plate devices or a LIBRA double knob cylinder, any card other than the Master will open after 2 orange flashing with beeps followed by the regular opening signal.

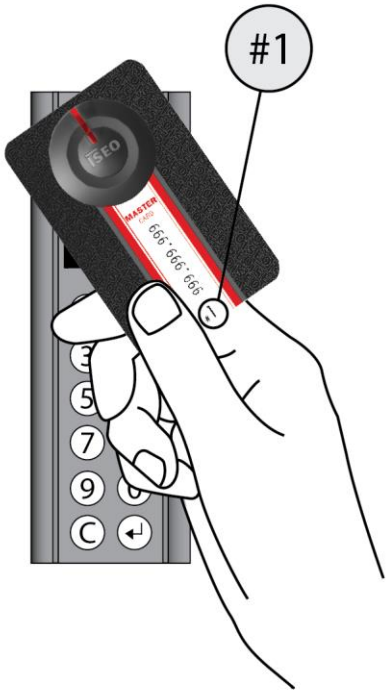
Opening signals of non-initialized ARIES handle plate devices or a LIBRA double knob cylinder

or any card other than Master

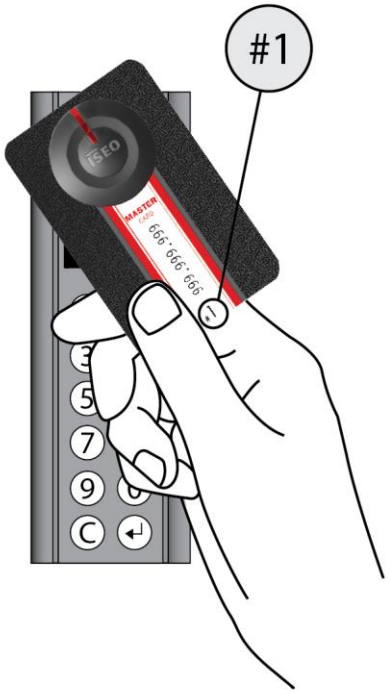
2 x 

Free passage, the actuator activated the opening.
The green light flashes for the default opening time

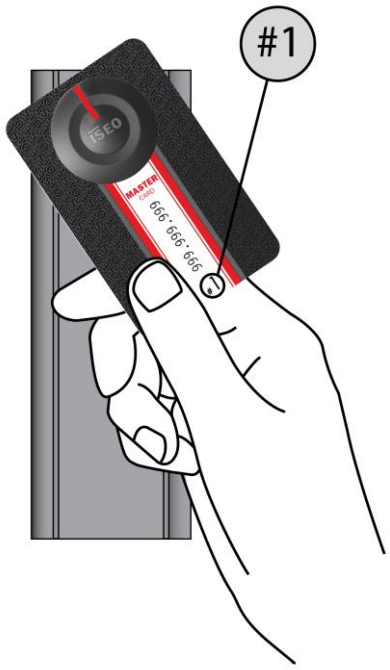
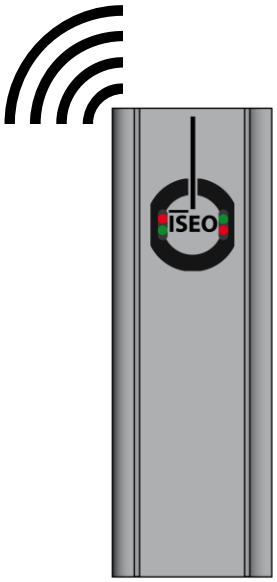
Initialization of the PAD ACD

Bring MASTER card **#1** closer to the device	The device emits 3 acoustic signals
	

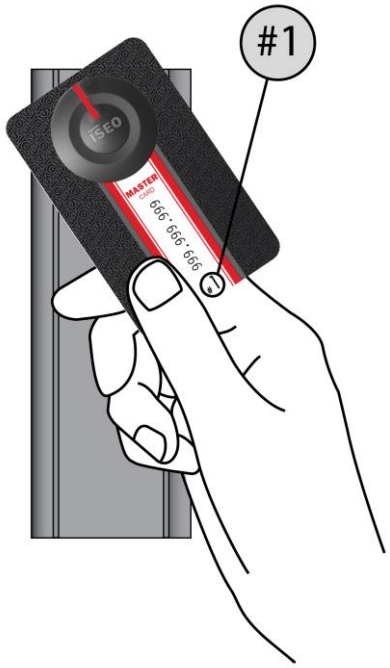
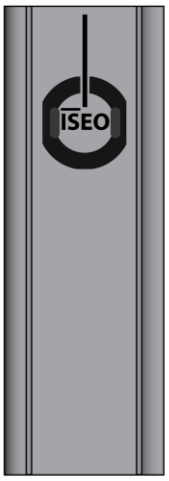
Checking of the initialization of the PAD ACD

Bring MASTER card **#1** closer to the device one more time	The menu appears on the device and the system was initialized with the system's code indicated on the SET of MASTER cards
	

Initialization of the STANDARD ACD

Bring MASTER card #1 closer to the device	The device emits 3 acoustic signals associated to 3 red/green light signals
	

Checking of the initialization of the STANDARD ACD

Bring MASTER card **#1** closer to the device one more time	The device turns off the blue lights waiting for commands, and the system was initialized with the system's code indicated on the SET of MASTER cards
	

Set-up methods of the devices' parameters

The set-up operations change according to the various devices, identified below as PAD with keyboard and display or STANDARD, with LIGHT indication.

In particular, the STANDARD device always requires the presentation of cards with specific programming sequences, while the PAD device can be programmed directly from the menu that appears by bringing closer the MASTER card.

1. **ADD:** to add a user card
2. **DELETE:** to delete a user card
3. **CLEAR:** to delete all user cards
4. **LOAD:** to program the SERVICE CARD
5. **UPDATE:** to update lost cards
6. **DISPLAY:** to visualize the WHITE LIST of the device
7. **READ:** to visualize the content of the WHITE LIST of another device
8. **OPTIONS:** to configure the options and set-up parameters

Set-up of the device's parameters

Set-up of the menu language (only PAD ACD)

8 OPTIONS 1 LANGUAG

The device can be configured in different languages, choose the required language, by inputting the matching number.

Sequence:

8 1 and choose the line corresponding to the required language, inputting the line's numeric value.

Set-up of the door's opening time (PAD ACD)

8 OPTIONS 2 TIME

In this section, it is possible to configure the door's opening time in seconds.

Sequence:

8 2 input the value in seconds and 

Set "0", corresponding to 100ms, for pulse opening systems.

Set-up of the door's opening time (STANDARD ACD)

In this section, it is possible to configure the door's opening time in seconds.

Sequence:

2 x 

Hold the SET UP card against the reader for the required amount of time (e.g. 3 x  = 3 seconds)

Bring it closer for less than one second, for pulse opening systems.

3 x 

Set-up of the keyboard's light (only PAD ACD)

8 OPTIONS 3 LIGHT

The keyboard's light can be adjusted from off to maximum luminosity, in 8 different degrees, by pushing button 1 to increase and button 2 to decrease luminosity. A sequence of three short acoustic signals close to each other, indicates that maximum or minimum luminosity has been reached.

Sequence:

8 3 … 1 to increase or 2 decrease … ↵

Compiling of the keyplan and input of the user's credentials

The user's credentials can be configured on the device with different functions, based on the type of door to control.

The special credentials requested during the input phase are:

- Very Important People V.I.P.+ credentials, it creates a privileged USER card, able to configure the door, only to be accessed with V.I.P. cards
- Very Important People V.I.P. credentials, it creates a privileged USER card, able to open the door, configured only to be accessed with V.I.P. cards
- Toggle credentials, it creates an additional function to the card, that allows to activate the office function.
- PIN, to achieve an improved security level, a PIN can be used consisting of 4 to 8 numbers that if input, it will be requested in addition to the opening credentials (only for PAD ACD).

For the operation of the V.I.P, V.I.P.+ and TOGGLE functions, refer to the *Special credentials* Chapter.

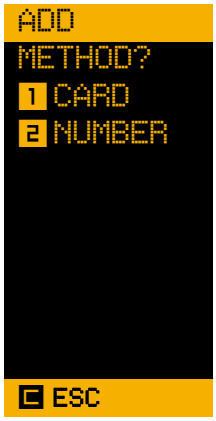
Note down the credentials, using the *Keyplan* annexed to the manual.

Each device can store maximum 150 USER cards

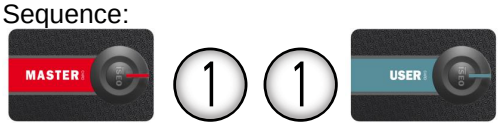
ADD of an USER Card (PAD ACD)

1 ADD

The procedure allows to add a USER card to the device.
The credential is added to the White List, choosing among two allowed procedures, by bringing closer and automatically acknowledging the card or by manually inputting the number, in case the card is not available. Each device can store maximum 150 USER cards.



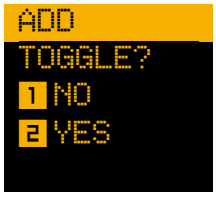
Sequence:



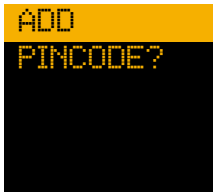
or

and input the number of the USER card to add

1 STANDARD, 2 V.I.P. . or 3 V.I.P.+



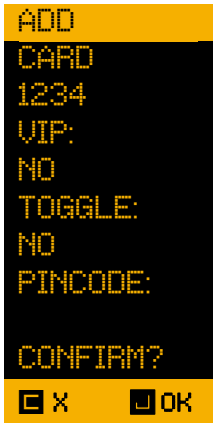
1 STANDARD or 2 TOGGLE



↵ if you do not want the PIN

or from 4 to 8 numbers to have an additional PIN and ↵ to confirm.

The summary screen follows



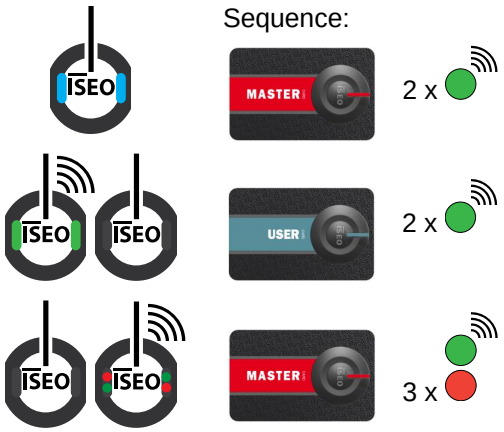
↵ to confirm

C to cancel the inputting

ADD of an USER Card (STANDARD ACD)

The procedure allows to add one or more USER cards to the device.
The credential is added to the White List. Each device can store maximum 150 USER cards.

Sequence:



To add Cards with enabled V.I.P., V.I.P.+ and/or TOGGLE functions, refer to chapter *Special credentials*.

Delivery of the credentials to the users

The stored USER cards can be delivered to the users, recording all the data on the keyplan

SIMPLY PAD - System Keyplan

			Access Control Devices																														
Seq.	Card_ID #1	User Name	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	#18	#19	#20	#21	#22	#23	#24	#25	#26	#27	#28	#29	#30
1	123	MARIO	X		X	X		X																								
2																																
3																																
4																																
5																																

The Keyplan is very important to manage credentials; we suggest to always keep it updated with card number, user name and devices in which the card was added.

In the example, Mario received USER card "123" which allows opening doors matched to devices no. 1, 3, 4 and 6.

In case of loss, the Keyplan remarkably facilitates the deletion and attribution process of new credentials.

To keep track of the stored cards, we suggest to adopt the following criterion:

"**X**" = card without V.I.P. and TOGGLE functions

"**T**" = card with TOGGLE function

"**V**" = card with V.I.P. function

"**V+**" = card with V.I.P.+ function

"**TV**" = card with TOGGLE and V.I.P. functions

"**TV+**" = card with TOGGLE and V.I.P.+ functions

How to use a Credential to open a door

Opening signals (PAD ACD)

Open door, the actuator have opened it.
The picture blinks during the opening time

Door not open. Opening refused.
Please refer to the Trouble shooting chapter for the signal motivation

Opening signals (STANDARD ACD)

Open door, the actuator have opened it.
The picture blinks during the opening time

o

Door not open. Opening refused.
Please refer to the Trouble shooting chapter for the signal motivation

Stand-by and Low Battery signals (only for ARIES electronic trim and LIBRA double knob cylinder)

STATUS	SIGNAL
Stand-by	No signal (electronic trim switch-off status)
Opening with low-battery status	blinking during the opening time
Opening with very low battery status	blinking for 3 seconds, then opening for the opening time
Opening with totally discarged battery	fixed for 3 seconds and then NO opening

WARNING: after the first low-battery signal change the batteries with new ones as soon as possible. Please refer to the device documentation for the type of batteries to be used.

Management of the system's and Keyplan updates

The Keyplan can be updated and modified anytime, but only by presenting the valid MASTER card.

The operations allowed are:

- ADD a new USER card in the White List of a device;
- DELETE an USER card in the White List of a device;
- DELETE all the USER cards in the White List of a device.

The changes to the Keyplan must always be recorded.

The ADD and DELETE operations can be performed according to different methods:

1. with USER Card;
2. with SERVICE card, in which the data of a lost or not available USER card have been copied through the PAD device;
3. using the keyboard, only with PAD access control devices

The SERVICE CARD is extremely useful to update the Keyplan, without recalling the relative USER cards, in case the user in not present.

It is mandatory to use the SERVICE CARD if the card to delete was lost or stolen (otherwise all cards present in the White List would require to be deleted and then added again) for STANDARD devices without keyboard and display.

Programming of the SERVICE CARD (only PAD ACD)

4 LOAD

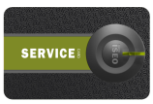
The image can be loaded on the SERVICE card, by doing a search between the USER cards loaded on the PAD device, or by inputting the credentials code of the USER card. Sequence:

4 1 input the number of row corresponding to the USER…

or

4 2 input the code of the USER card and … …

Bring closer the SERVICE CARD…



…

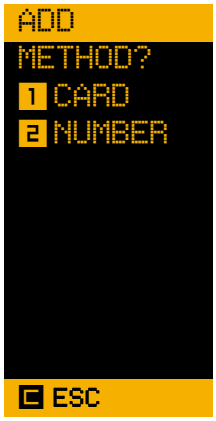
3 consecutive acoustic signals confirm the image has been copied.

The SERVICE CARD is now programmed with the code of the USER Card to manage. With the SERVICE CARD, it is possible to carry out input, edit and delete operations of the USER card on the devices, but it will not be possible to open the door. The SERVICE CARD is not enabled to control the opening; its only function is to transfer credentials between devices.

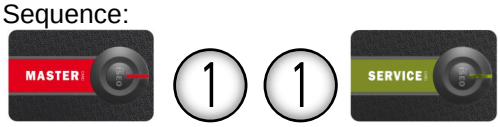
ADD of an USER Card through the SERVICE CARD (PAD ACD)

1 ADD

The procedure allows to add a USER card to the device.
The credential is added to the White List, choosing among two allowed procedures, by bringing closer and automatically acknowledge the card or by manually inputting the number, in case the card is not available.

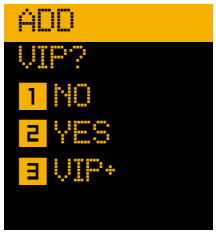


Sequence:

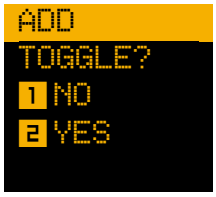


or

and input the number of the USER card to add



1 STANDARD, 2 V.I.P. . or 3 V.I.P.+

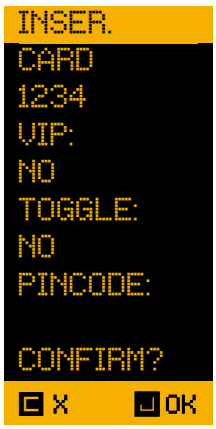


1 STANDARD or 2 TOGGLE

↵ if you do not want to input the PIN

or from 4 to 8 numbers to have an additional PIN and ↵ to confirm.

The summary screen follows



↵ to confirm

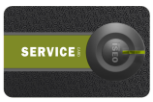
C to cancel the inputting

ADD of an USER Card through the SERVICE CARD (STANDARD ACD)

The procedure allows to add a USER card to the device.
The credential is added to the White List.

Sequence:

2 x 



2 x 

(it is possible to input more USER cards, by bringing them closer in sequence)

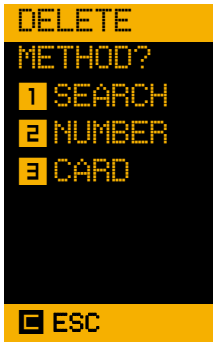
3 x 

after a 10 sec Timeout the sequence is closed automatically

To add Cards with enabled V.I.P., V.I.P.+ and/or TOGGLE functions, refer to chapter *Special Credentials*.

Deletion of a USER Card (PAD ACD)

2 DELETE

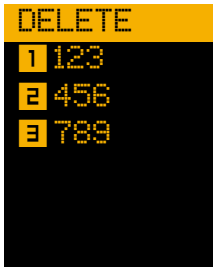


The procedure deletes a USER card from the White List of the device. The credentials can be deleted in various way, searching for the code among the stored cards, inputting the code to delete or bringing closer the USER card or SERVICE card to delete.

Sequence:

2

THEREFORE



1 and input the number of row corresponding to the code to delete and ↵ to confirm. To browse the screens, use buttons ↵ e 0

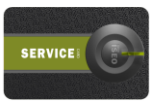
for example: input 3 and ↵ to delete the card with code “789”

OR

2 input the code of the card to delete and ↵ ↵ to confirm

OR

3 

or 

corresponding to the code to delete and ↵ to confirm

Deletion of a USER Card (STANDARD ACD)

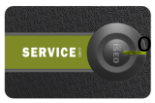
The procedure deletes a USER card from the White List of the device.
To delete the credential, you must have the USER Card to delete or the SERVICE Card with the image of the USER card to delete.

The SERVICE CARD must be programmed with the PAD ACD, as described in chapter *"Programming of the SERVICE CARD (only PAD ACD)".*

Sequence:

2 x

4 x

or


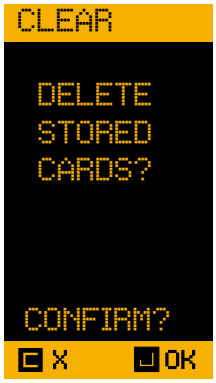
2 x (it is possible to delete more USER cards, bringing them closer in sequence)

3 x after a 10-sec Timeout, the sequence is closed automatically

Deletion of all USER Cards and clearing of the White List (PAD ACD)

3 CLEAR

The procedure deletes all USER cards from the White List of the device.



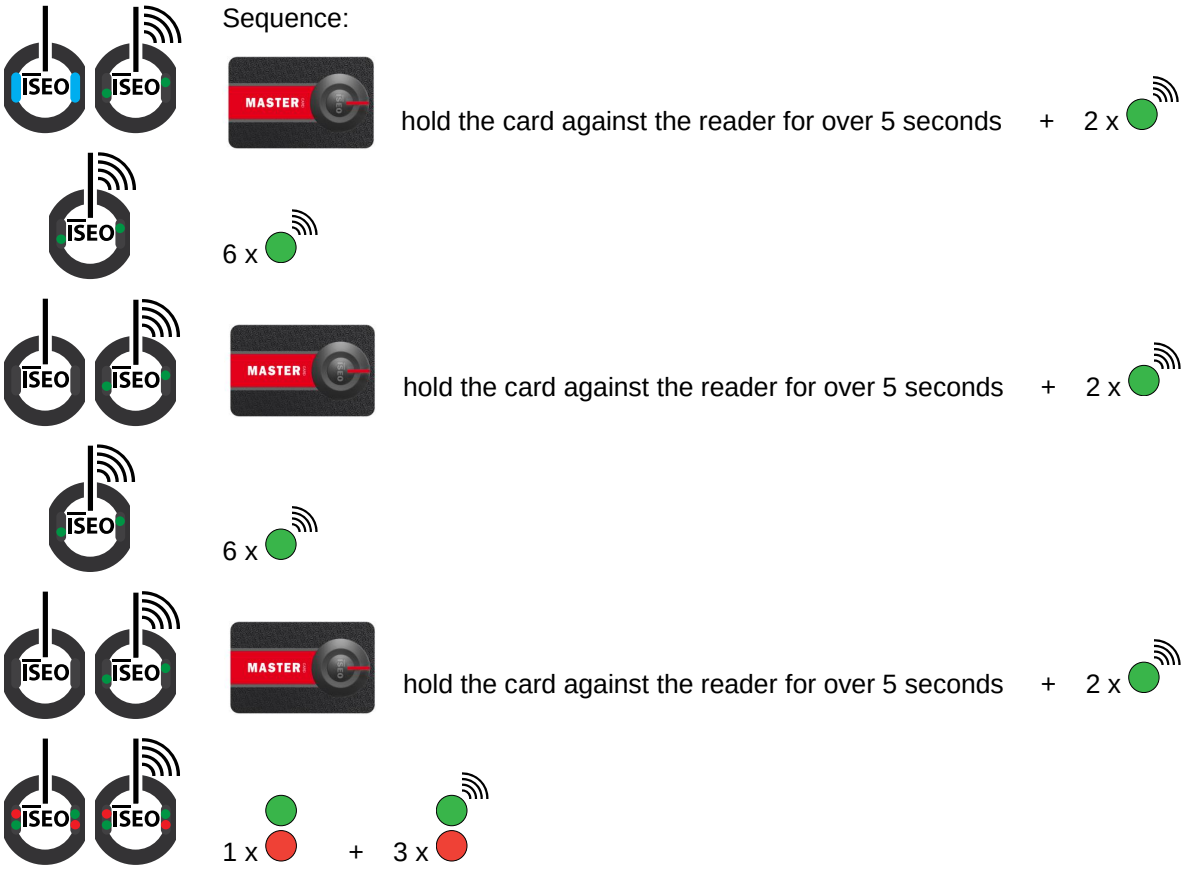
Sequence:

 to confirm

 to cancel the inputting

Deletion of all USER Cards and clearing of the White List (STANDARD ACD)

Also in the standard device, it is possible to completely clear the White List, by deleting all the input cards in one single operation. To carry out the operation, you must need the valid MASTER card, which must be brought closer to the device 3 times in a row, for over 5 seconds each time. Acoustic and light signals guide the execution times.



Updating of a lost or stolen card

If a USER card is lost or stolen, you must:

- deliver a new USER Card to the user (with the same access rights of the previous one)
- inhibit immediately the operation of the old USER Card in all the relevant devices.

This operation can be performed in two ways;

1. By deleting the lost USER Card (through a SERVICE CARD with the relative image loaded) and by adding the new USER Card in all the relevant devices, following in sequence, chapters:
   - *Programming of the SERVICE CARD (only PAD ACD)*
   - *Deletion of a USER Card (PAD and STANDARD ACD)*
   - *ADD of the USER Card (PAD ACD)*
2. Update of the new USER Card with the image of the lost USER Card on PAD ACD, and then simply using the new USER card in all relative system's devices, at least once.

The second option is much simpler and quicker, since it is not required to physically update the White Lists of all devices in object, but you just need to load the image of the USER Card to be replaced in the new USER Card, through the PAD ACD.

5 UPDATE

In order to update a lost USER card, you must first of all, create the image on a new USER Card, using the PAD device.

Sequence:

5 and choose among the following three options:

1. SEARCH, to search the USER Card among those stored in the device
2. NUMBER, to input directly the number of the USER card to update
3. RESET to reset the USER Card to its initial status and remove the update information, see chapter: *Resetting the USER Card (PAD ACD)*

SEARCH:

1 and input the number of the row corresponding to the code to update and ↵ to confirm. To browse the screens, use buttons ↵ and 0

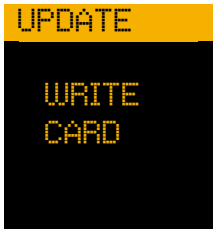
for example: input 3 and ↵ to update the card with code “789”

OR

NUMBER:

2 input the code of the card to update and ↵ ↵ to confirm

and continue with writing the image



3 acoustic signals confirm the reading of the new USER Card

The message on the display and 3 acoustic signals confirm the reading of the new USER Card

IMPORTANT: update all the system’s devices using the new Card on the devices in object, at least once. Refer to the Keyplan to know the devices and to the following chapters, for the procedure to follow on PAD and STANDARD ACD.

Updating of a PAD device with updated USER card

Bring closer to the device, the new card with the image of the lost USER card, the display informs you that the device is updating. Once this operation is concluded, it emits 4 acoustic signals.

Updating of a STANDARD device with updated USER card

new card with the image of the lost USER Card

4 x .

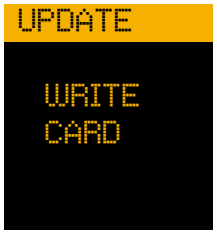
Resetting of a USER Card (PAD ACD)

5 UPDATE

This procedure allows to restore the initial status of a USER Card used to update a lost card, by deleting the image used for updating. We suggest to perform this function if you find lost cards, which configuration is unknown.

Sequence:

5 and choose the option 3



Bring closer to the device, the USER Card to reset

3 acoustic signals confirm the reading of the new USER Card

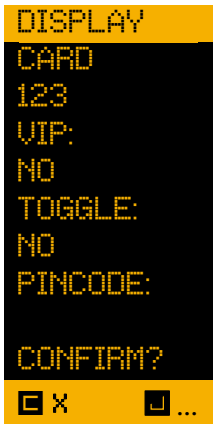
Visualization of the stored cards (PAD ACD)

6 DISPLAY

It allows to visualize the list of credentials stored in the device, and change the special functions.
Sequence:

6

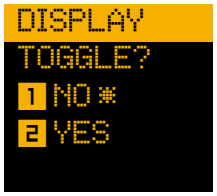
To browse the screens, use buttons ↵ and 0



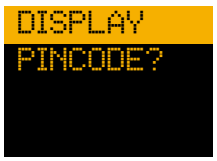
If you want to change the special functions of a stored card, input the number of row corresponding to the code to modify and ↵ to confirm.

Press ↵ on the summary screen of the Card, to begin editing

1 STANDARD, 2 V.I.P., 3 V.I.P.+ or ↵ to leave the current set-up (*)

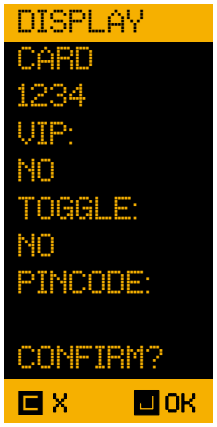


1 STANDARD, 2 TOGGLE or ↵ to leave the current set-up (*)



↵ if you do not want to edit the PIN

or input from 4 to 8 numbers for a new PIN and ↵ to confirm.



The summary screen follows

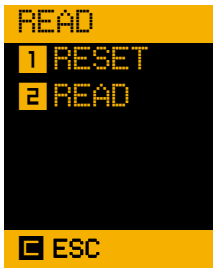
↵ to confirm

C to cancel the inputting

Reading of the White List through SERVICE CARD

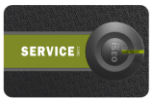
There is the possibility to read the content of the White List of a STANDARD ACD, acquiring the content through SERVICE CARD and submit it to a PAD device for reading.

7 READ

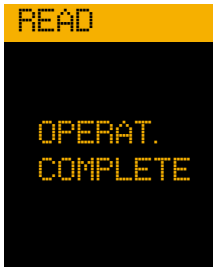


The first operation to perform is to clear the content of the SERVICE CARD with PAD device.

Sequence:



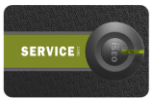
Bring closer to the device, the SERVICE Card to reset



3 acoustic signals confirm the resetting of new SERVICE Card

The SERVICE card is now ready to read the White List of the standard device, which must be brought closer to execute the transfer.

Sequence:



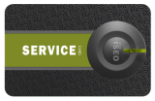
hold the card in front of the device until the notice that the card reading operation has been completed, appears (the operation can take a few seconds)

1 x + 3 x

Return to the PAD device and read the content of the SERVICE CARD, corresponding to the content of the STANDARD device just acquired.

Sequence:

7 2

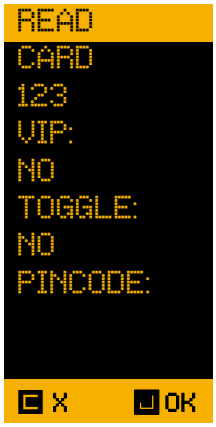


Bring closer to the device, the SERVICE Card to read

The display shows the White List

To browse the screens, use buttons and 0

To know about a credential, input the number of row corresponding to the code to visualize in details



Press on the summary screen to return to the list

Copy of the White List through SERVICE CARD

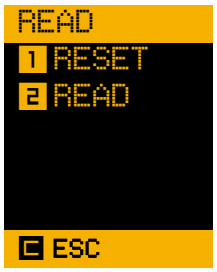
In case more system's devices require the same access rights, the entire White List can be copied from one device to another through SERVICE CARD.

The copy procedure of the White List must be performed following the steps below:

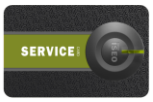
1. initialize the SERVICE CARD
2. delete the White List of all the devices on which the new White List must be copied
3. read the White List from the device to copy
4. copy the White List on the new devices

Each SERVICE CARD contains one White List at a time. In case different White Lists must be copied, repeat the procedure from point 1 for each White List to copy.

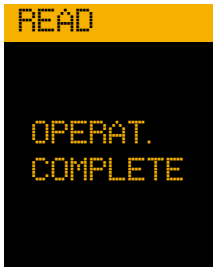
Initialize the SERVICE CARD



Sequence:



Bring closer the SERVICE CARD to empty to the device



3 sound signals confirm that the SERVICE CARD has been reset

Deletion of the White List from devices (PAD ACD)

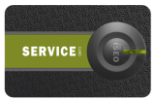
Refer to chapter "Deletion of all USER cards and clearing of the White List (PAD ACD)".

Deletion of the White List from devices (STANDARD ACD)

Refer to chapter "Deletion of all USER cards and clearing of the White List (STANDARD ACD)"

Reading of the White List from devices (PAD ACD)

Sequence:

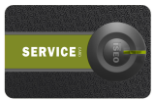


hold the card in front of the device until the waiting signal stops and the sound signals are enabled (the operation may lasts a few seconds)

3 x

Reading of the White List from devices (STANDARD ACD)

Sequence:

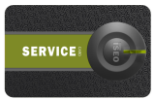


hold the card in front of the device until the card writing end message is displayed (the operation may lasts a few seconds)

1 x + 3 x

Copy the White List on the new devices (PAD ACD)

Sequence:



Bring closer the SERVICE CARD to read to the device

hold the card in front of the device until the waiting signal stops and the sound signals are enabled (the operation may lasts a few seconds)

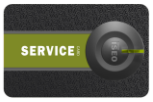
3 x

Copy the White List on the new devices (STANDARD ACD)

Sequence:

hold the card for more than 5 seconds + 2 x

6 x



hold the card in front of the device until the waiting signal stops and the sound signals are enabled (the operation may lasts a few seconds)

1 x + 3 x

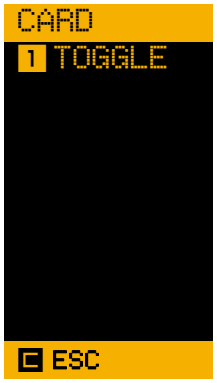
Special credentials

TOGGLE credential

The TOGGLE Card has the function to authorise a USER Card to perform the Toggle Mode function, also called “office function”.

The USER cards with this function activated, can enable the fixed opening of the door. To close the door repeat the same sequence.

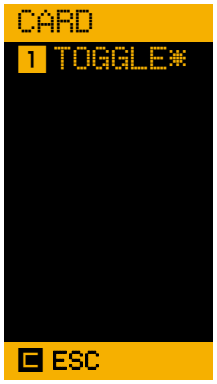
Opening of a door in TOGGLE – Office mode (PAD ACD)



Opening sequence:

The door remains open up to the closing sequence

Closing of a door in TOGGLE – Office mode (PAD ACD)



Closing sequence:

The door is closed

If the TOGGLE function is not used, the door will open after 2 seconds in normal mode, for the opening time.

Opening of a door in TOGGLE – Office mode (STANDARD ACD)

Opening sequence:

Hold the card against the reader for at least 3 seconds

3 x

Open door

Closing of a door in TOGGLE – Office mode (STANDARD ACD)

Closing sequence:

Hold the card against the reader for at least 3 seconds

5 x

Closed door

If the USER Card with TOGGLE mode is brought closer to the standard device for less than 3 seconds, the door opens in normal mode, for the opening time.

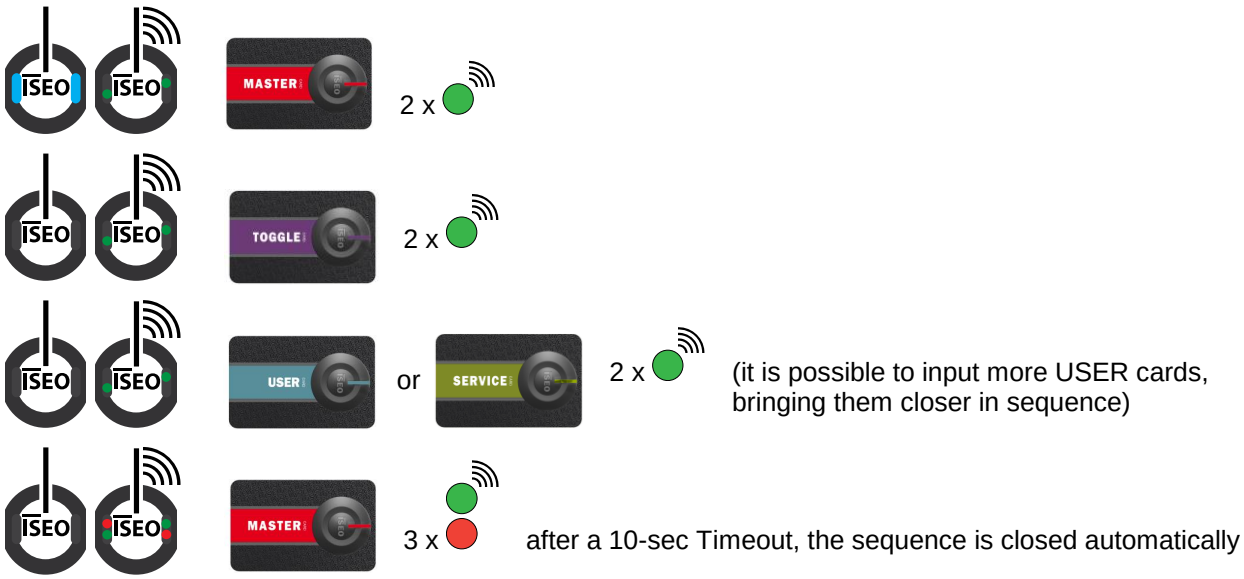
ADD of the USER Card with TOGGLE mode (PAD ACD)

In the PAD device, the special functions are always requested during the storing phase of the USER card, therefore please refer to chapter: *ADD of an USER card (PAD ACD)*

ADD of the USER Card with TOGGLE mode (STANDARD ACD)

The procedure allows to add a USER card with TOGGLE mode, to the standard device.
The credential is added to the White List.

Sequence:

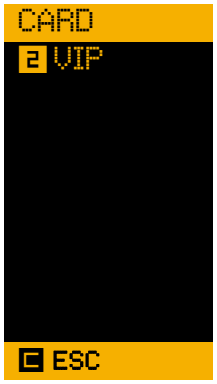


V.I.P.+ (Very Important People +) credential

The V.I.P.+ credential creates, if enabled, a higher class of the USER Card, with the possibility to authorise or non-authorise access to the door to standard USER Cards, or with disabled V.I.P or V.I.P.+ mode.

The function can be enabled and disabled at the door, any time.

Activation of the V.I.P. – Very Important People mode (PAD ACD)



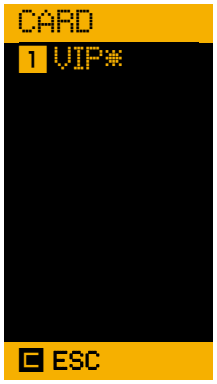
Activation sequence:

2

CARD WITH V.I.P.+ MODE ENABLED

The door can be accessed only with USER cards with enabled V.I.P function

Deactivation of the V.I.P. – Very Important People mode (PAD ACD)



Deactivation sequence:

2

CARD WITH V.I.P.+ MODE ENABLED

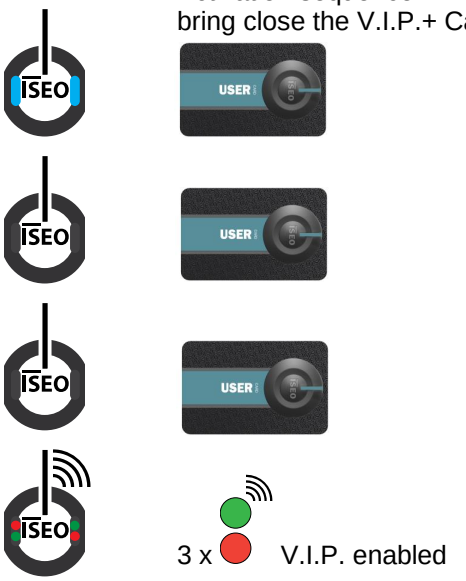
The door can be accessed again with all stored USER Cards

If the V.I.P.+ function is not used, the door will open after 2 seconds in normal mode, for the opening time.

The enabling of the V.I.P. mode does not delete the USER cards without V.I.P function from the White List, but disables them temporarily.

Activation of the V.I.P. – Very Important People mode (STANDARD ACD)

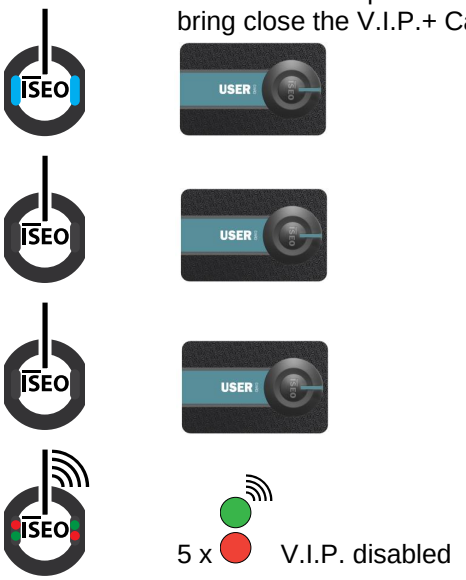
Activation sequence:
bring close the V.I.P.+ Card for 3 times in less than 6 seconds



3 x V.I.P. enabled

Deactivation of the V.I.P. – Very Important People mode (STANDARD ACD)

Deactivation sequence:
bring close the V.I.P.+ Card for 3 times in less than 6 seconds



5 x V.I.P. disabled

If the USER Card with V.I.P.+ credential is brought close to the device one time only, the door remains in its current mode and opens for the opening time.

The enabling of the V.I.P. mode does not delete the USER cards without V.I.P function from the White List, but disables them temporarily.

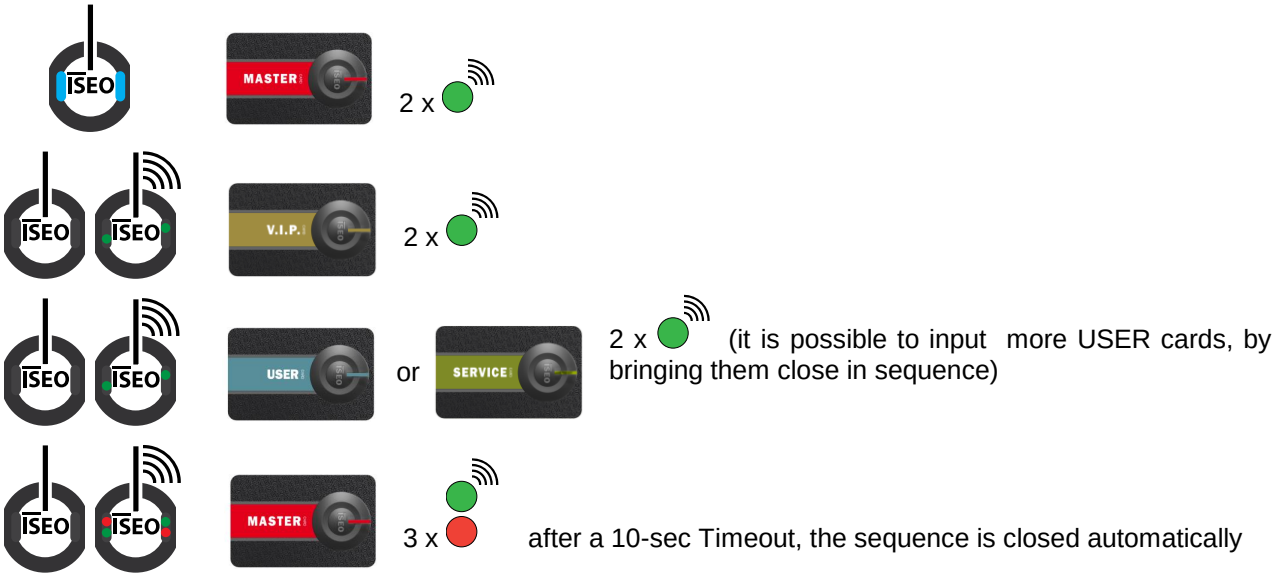
ADD of the USER Card with V.I.P. or V.I.P.+ mode (PAD ACD)

In the PAD device, the special functions are always requested during the adding phase of the USER card, therefore please refer to chapter: *ADD of an USER Card (PAD ACD)*.

ADD of the USER Card with V.I.P. mode (STANDARD ACD)

The procedure allows to add a USER card with V.I.P mode, to the standard device.
The credential is added to the White List.

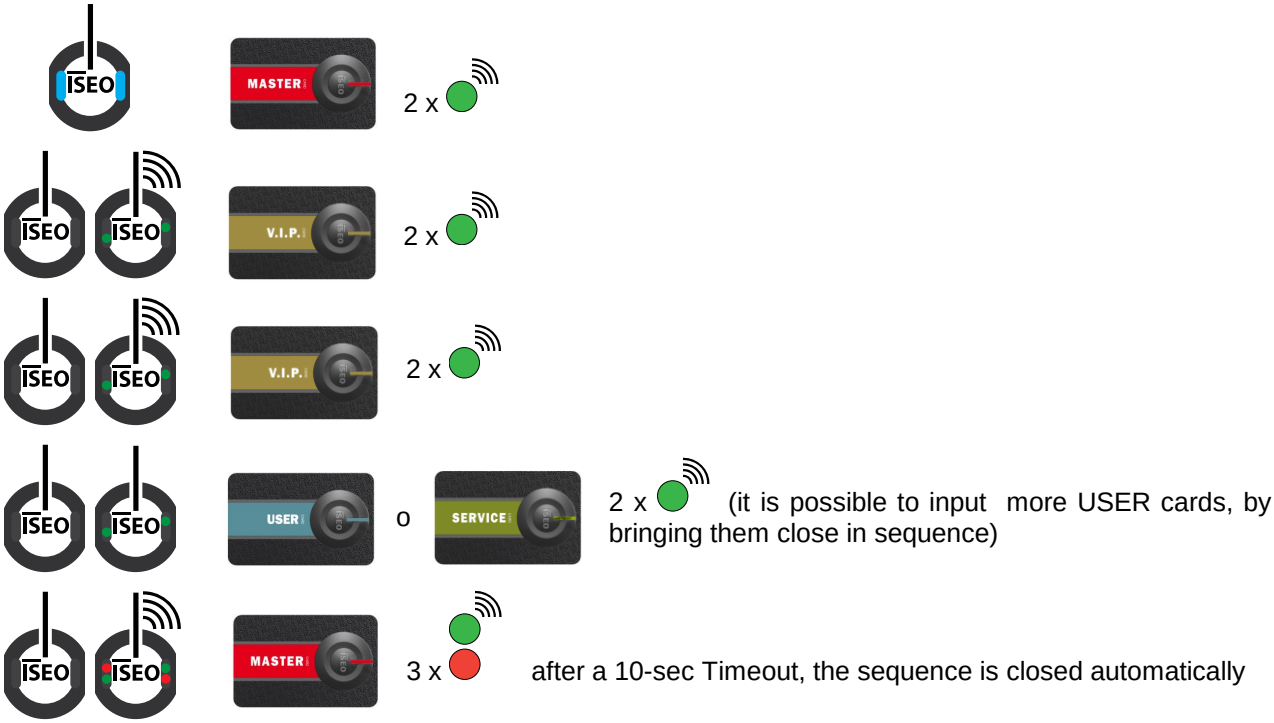
Sequence:



ADD of the USER Card with V.I.P.+ mode (STANDARD ACD)

The procedure allows to add a USER card with V.I.P.+ mode, to the standard device.
The credential is added to the White List.

Sequence:



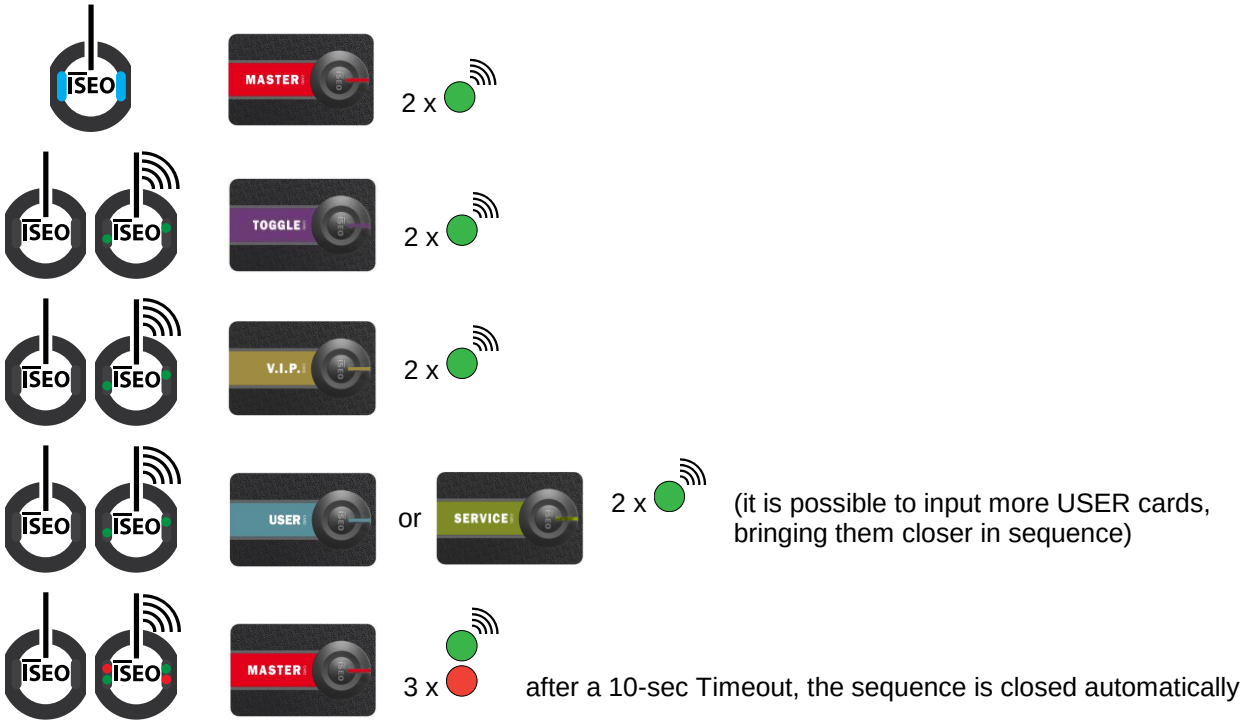
ADD of the USER Card with TOGGLE and V.I.P. or V.I.P.+ mode (PAD ACD)

In the PAD device, the special functions codes are always requested during the adding phase of the USER card, therefore please refer to chapter: *ADD of an USER (PAD ACD)*.

ADD of the USER Card with TOGGLE and V.I.P. mode (STANDARD ACD)

The procedure allows to add a USER card with TOGGLE and V.I.P modes, to the standard device.
The credential is added to the White List.

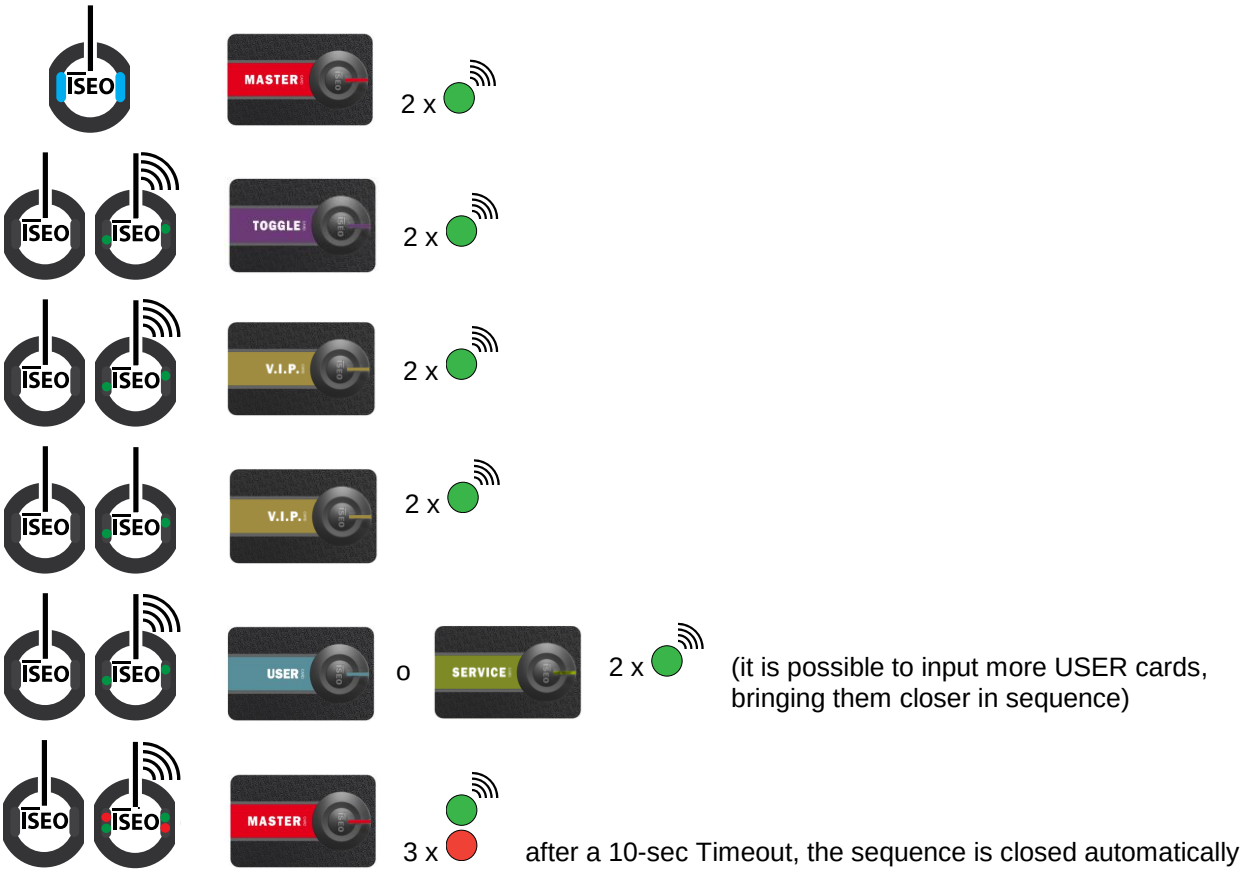
Sequence:



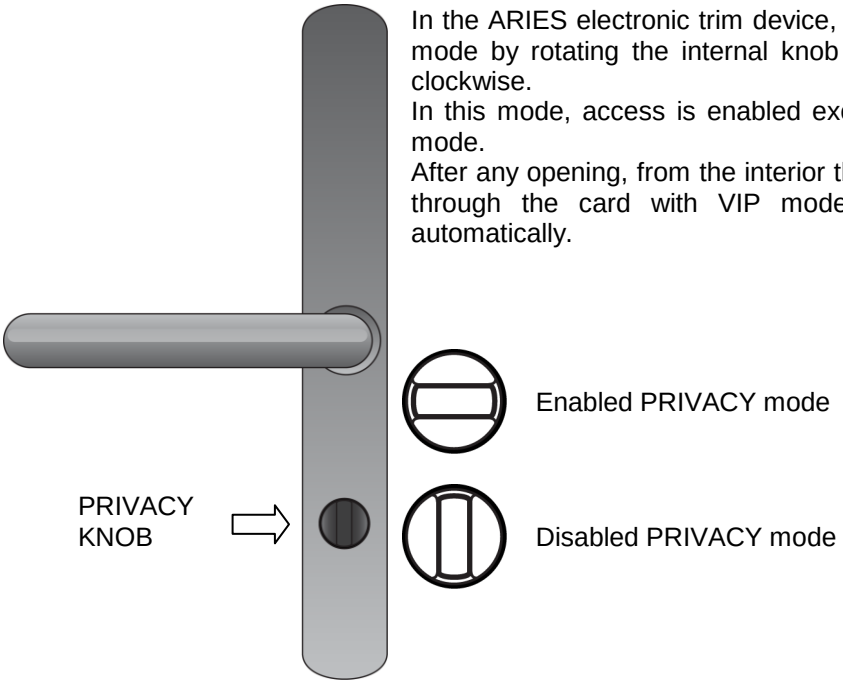
ADD of the USER Card with TOGGLE and V.I.P.+ mode (STANDARD ACD)

The procedure allows to add a USER card with TOGGLE and V.I.P.+ modes, to the standard device.
The credential is added to the White List.

Sequence:



PRIVACY mode (only for the ARIES electronic trim device)



In the ARIES electronic trim device, it is possible to activate the PRIVACY mode by rotating the internal knob by 90 degrees clockwise or counter clockwise.
In this mode, access is enabled exclusively to the cards stored with VIP mode.
After any opening, from the interior through the handle or from the exterior through the card with VIP mode, the PRIVACY mode is disabled automatically.

Signal of the mechanical override usage (only for ARIES electronic trim)

When the mechanical override cylinder is used to open, the ELECTRONIC TRIM detects and stores in its memory the opening mode. Then, at each following opening, a special signal is displayed to show that the emergency override has been used.


6 x followed by the standard signals and opening

The mechanical override usage signal stays until it will be reset.
To reset the mechanical override signal follow this procedure:

hold the card against the reader for at least 5 seconds

2 x + 3 x

Updating of the MASTER card (in case of loss or theft)

If a MASTER Card is lost or stolen, in order to disable it, just use the following MASTER card of the same SET of MASTER credentials, on the device.

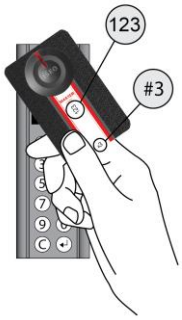
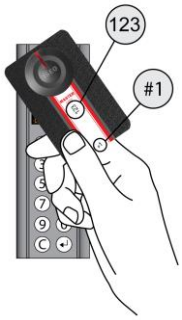
- By bringing MASTER card #2 closer to the device, MASTER card #1 is disabled.
- By bringing MASTER card #3 closer to the device, MASTER cards #2 and #1 are disabled.

WARNING

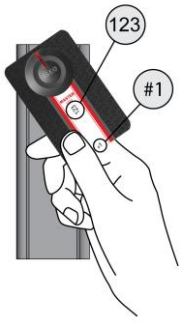
Authenticate the MASTER card of higher number only if the card of lower number has been lost or stolen, since the authentication of a MASTER card will disable the MASTER cards of lower number.

In case the MASTER card of lower number is disabled by mistake, this can be re-activated by bringing the active MASTER card of higher number closer, and then the MASTER card of lower number of the same system code, that needs to be re-activated.

Re-activation sequence of the MASTER Card of lower number (PAD ACD)

Bring closer the MASTER card of higher number to the device. #3 re-activates #2 and #1 #2 re-activates #1	The menu appears on the device	Bring closer the MASTER card of lower number belonging to the same SET	Remove the card and wait until three sound signals are emitted. The display during the updating phase	The logo appears on the display and the card of lower number has been reset on the device
				

Re-activation sequence of the MASTER Card of lower number (STANDARD ACD)

Bring closer the MASTER card of higher number to the device. #3 re-activates #2 and #1 #2 re-activates #1	The lights of the device are disabled	Bring closer the MASTER card of lower number belonging to the same SET	Remove the card and wait until three sound signals are emitted and the red/green lights are turned on	The blue lights are enabled and the card of lower number has been reset on the device
				

All PAD ACD and STANDARD ACD devices present in the system must be updated with the new MASTER Card.

LOSS OF MATER CARDS #1 AND #2

In case of loss of MASTER cards #1 and #2 and subsequent authentication of the system with MASTER card #3, we suggest to immediately acquire a new SET of MASTER credentials and update the system with the new SET.

MASTER card #3 must be considered as the updating card for the new SET, since its loss could **irreversibly** compromise the possibility to modify or update the system.

Modification of the SET of MASTER credentials and updating of the system's code

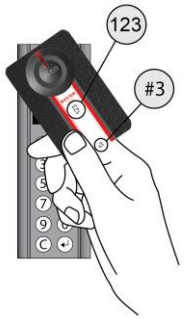
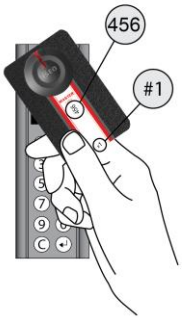
If both MASTER cards #1 and #2 are lost, in order to ensure the system's security, you must update the system's devices with a new SET of MASTER credentials (**if MASTER card #3 is lost, it will not be longer possible to operate on the system's devices).**

The connection to the devices of the new SET of MASTER credentials is carried out using MASTER card #3 of the old SET on the devices, followed by MASTER card #1 of the new SET.

No change is made to the User's List of the devices.

All PAD ACD and STANDARD ACD devices present in the system must be updated with the new system's code.

Updating sequence of the system's code (PAD ACD)

Bring MASTER card **#3** closer to the device	The menu appears on the device	Bring closer MASTER card #1 of the new SET	Remove the card and wait to hear three acoustic signals. The display on the updating phase	The logo appears on the display and the new SET with the new system's code was updated on the device
				

Updating sequence of the system's code (STANDARD ACD)

Bring MASTER card **#3** closer to the device	The lights of the device turn off	Bring closer MASTER card **#1** of the new SET	Remove the card and wait to hear the three acoustic signals when the red/green lights turn on	The blue light turns on and the new SET with the new system's code was updated on the device
				

Keyplan table

SIMPLY PAD - System Keyplan

Access Control Devices

Seq.	Card_ID #1	User Name	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	#18	#19	#20	#21	#22	#23	#24	#25	#26	#27	#28	#29	#30
1																																
2																																
3																																
4																																
5																																
6																																
7																																
8																																
9																																
10																																
11																																
12																																
13																																
14																																
15																																
16																																
17																																
18																																
19																																
20																																
21																																
22																																
23																																
24																																
25																																

Glossary

Access Control:	system of electronic and/or mechanical devices to allow selective access through the users' doors.
Door:	passage or door which access is electronically controlled by the ACD (access control devices).
Credential:	device that allows to identify the user and authorise or non-authorise access through a door (in general, a card or contactless Card).
Contactless card:	electronic card that can be read by the access control device, by simply bringing it closer to the same, without physical contact.
Keyplan:	matrix of the doors and user cards to register the authorised users and relative doors.
PAD ACD:	electronic access control device equipped with contactless card reader, keyboard and display.
Standard ACD:	electronic access control device equipped with contactless card reader and signalling lights.
MASTER Card	contactless card used to program the system.
USER Card:	contactless card used to open one or more doors.
V.I.P. Card:	contactless card used to enable the V.I.P or V.I.P.+ function to USER cards for one or more doors.
TOGGLE Card:	contactless card used to enable the Toggle function (or office function) to USER cards for one or more doors.
SET-UP card:	contactless card used to set-up the opening time of an access control device.
White List:	list of USER cards enabled to open an access control device.
Timout:	time after which an action will automatically take place.
Menu:	list of functions visualized on the display, which are possible to select by pressing the relative numeric key.
Opening time:	time during which a door remains open following a standard opening through USER card.

Trouble Shooting

Common for all the devices

PAD ACD	STANDARD ACD	
 FIXED	 FIXED	**Effect** Opening not possible **Possible cause** Communication error **What to check** Check the power supply of all the gate devices **What to do** - Remove and provide again power upply - Try to repeat the exchange of coded keys procedure(see system's configuration manual) - Contact ISEO Zero1 technical assistance
 BLINKING	 FIXED	**Effect** Opening not possible **Possible cause** The opening is forbidden **What to check** If there actuators with interlock function one of them is still open **What to do** - Remove and provide again power upply - Contact ISEO Zero1 technical assistance
 BLINKING	 FIXED	**Effect** The door remains in open position **Possible cause** The door remains in open position **What to check** The TOGGLE function have been activated **What to do** Remove the TOGGLE function

Special only for ARIES electronic trim and LIBRA double knob cylinder

 2 BLINKING with BEEP	**Effect** Opening not possible **Possible cause** Privacy mode active **What to do** Use an USER card with VIP function active
 BLINKING	**Effect** Opening but with the orange signal **Possible cause** Low batteries **What to do** Change the batteries as soon as possible
 BLINKING	**Effect** Delayed opening after 3 seconds signal **Possible cause** Very low batteries **What to do** Change the batteries immediately.
 FIXED	**Effect** Opening not possible after the 3 seconds signal **Possible cause** Totally discharged batteries **What to do** Open with emergency override cylinder of emergency power supply and then change the batteries immediately.

Special only for ARIES

 6 BLINKING	**Effect** The device emits 6 blinking **Possible cause** The mechanical override cylinder has been used to open **What to do** Reset the mechanical override usage signal as explained at page 33.

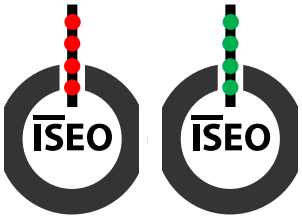
Signals following the change of battery

for ARIES handle plate devices and LIBRA double knob cylinder

When a new battery is introduced in ARIES handle plate devices or a LIBRA double knob cylinder, an automatic procedure is performed that eliminates the passivation layer.

Status:

After introducing and connecting the new battery to the device.

 VARIABLE SIGNALS	The device begins the automatic procedure to eliminate the passivation layer that may last a few minutes, emitting variable signals
 ALTERNATING FLASH	At the end of the procedure, the device flashes in red and green, alternatively, for at least 5 seconds.

Wait until the procedure is completed, without removing the battery.

The duration of the procedure does not provide any information and does not depend on the efficiency of the battery.

ISEO®

www.iseo.com

Iseo Serrature s.p.a.
Via San Girolamo 13
25055 Pisogne (BS)
Italy
Tel +39 0364 8821
Fax +39 0364 882263
iseo@iseo.com

Fiam s.r.l.
Via Don Fasola 4
22069 Rovellasca (CO)
Italy
Tel +39 02 96740420
Fax +39 02 96740309
www.fiamserrature.it

ISEO Zero1
ELECTRONIC SUPPORT SERVICE
iseozero1@iseo.com