USER MANUAL

ACCESS CONTROL SYSTEM
SIMPLY SEQUENCE
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

The rights concerning all technologies and products which are part of this device, belong to the relative holders.

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

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.

Any combination between the available devices is accepted in a system configured with Simply SEQUENCE system, in compliance with the configuration rules, as described in the system's configuration manual, available in the download area of ISEO serrature's website at: http://www.iseoserrature.com.

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

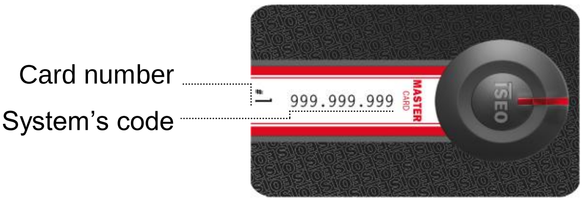
The credentials used in the system can be functionally divided in:

	MASTER Card used to “configure” and “manage” the access control system
	USER Card used by the users to “open” doors
USER PINCODE	**USER Pincode** Numeric code from 4 to 8 digits (only PAD ACD)
	SPECIAL Cards (SET UP, TOGGLE, VIP) used to enable special doors’ functions

SET OF MASTER Credentials for the SIMPLY SEQUENCE 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. Use of the Credentials
   - types of credentials
   - channels mechanism
   - code blocked, wrong credentials
4. 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.

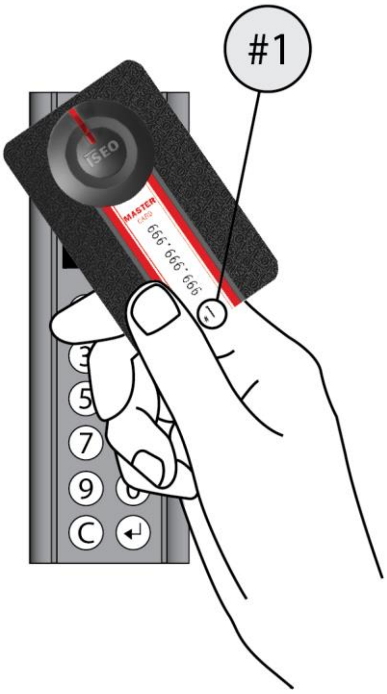
Opening signals of non-initialized ARIES handle plate devices or a LIBRA double knob cylinder

or any card other than Master

2 x ●

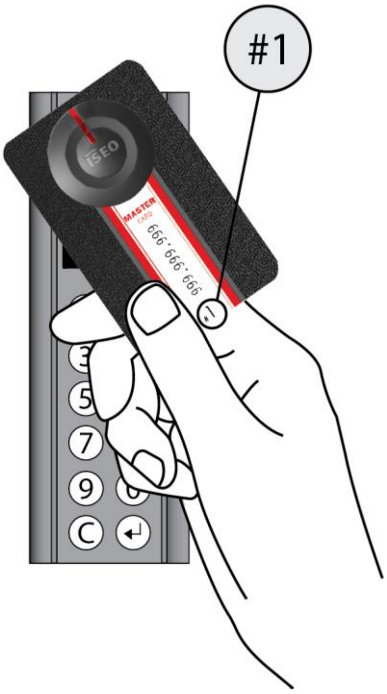
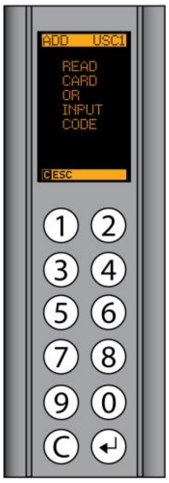
● Free passage, the actuator activated the opening.
The green light flashes for the default opening time

Initialization of the PAD ACD

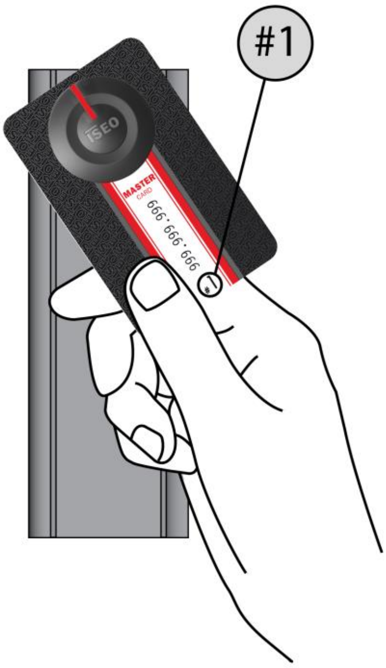
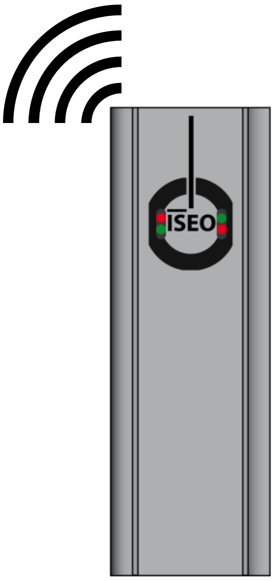
Bring MASTER card **#1** closer to the device 	The device emits 3 acoustic signals

#1
MASTER CARD
999.999.999
1

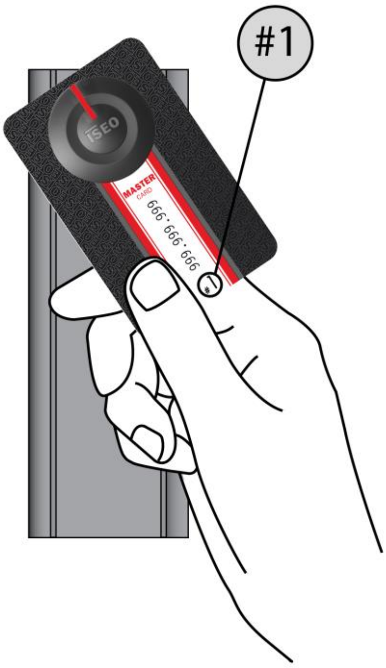
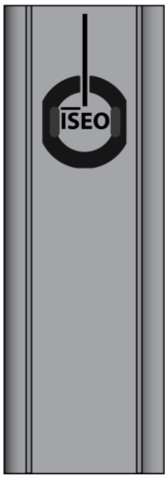
Checking of the initialization of the PAD ACD

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

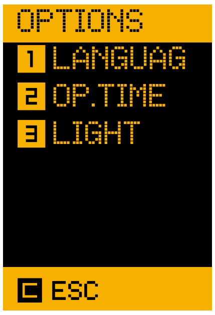
The set-up operations change according to the various devices, identified below as PAD with keyboard and display or STANDARD, with LIGHT indication.

For the PAD device, the functional parameters can be programmed directly from the menu, that can be activated through MASTER card.

The STANDARD device always requires to present the cards according to specific sequences and programming times.

Set-up of the device’s parameters

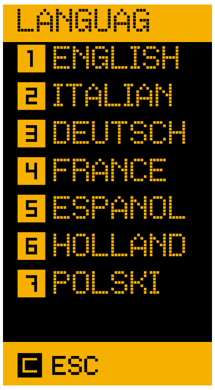
Set-up of the menu OPTIONS (only PAD ACD)


OPTIONS
1 LANGUAG
2 OP.TIME
3 LIGHT
C ESC

3 x

1. **LANGUAG:** language of the menu
2. **OP. TIME:** opening time in seconds
3. **LIGHT:** keypad light settings

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


LANGUAG
1 ENGLISH
2 ITALIAN
3 DEUTSCH
4 FRANCE
5 ESPANOL
6 HOLLAND
7 POLSKI
C ESC

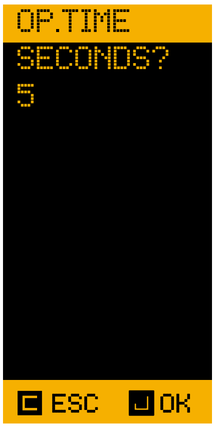
The device can be configured in different languages, choose the required language, by inputting the matching number.

Sequence:

3 x

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)


OP.TIME
SECONDS?
5
C ESC ↵ OK

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

Sequence:

3 x

② , input the value in seconds and ↵

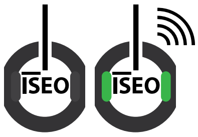
Set “0”, corresponding to 100ms, for pulse opening systems.

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 🟢



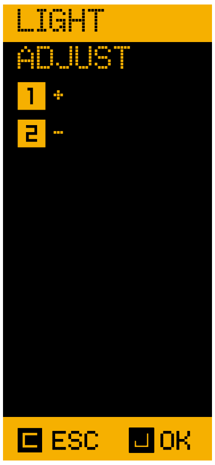
🟢 Hold the SET UP card against the reader for the required amount of time (e.g. 3 x 🟢 = 3 seconds)

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

🟢

3 x 🔴

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



LIGHT
ADJUST
1 +
2 -
ESC OK

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:

3 x

3 … 1 to increase or 2 to decrease… ↵

Compatible USER cards

A USER card (or tag) can be:

- ISEO card (proprietory cards);
- a badge issued by a third party, already present in the user’s structure (e.g. cards for the users’ authorised access).
- A code from 4 to 8 digits (only PAD ACD)

❗ The MASTER and SPECIAL cards cannot be third party’s but only ISEO cards.

The readers are able to read the following types of cards as USER cards:

- Mifare Classic (ISO14443A);
- Mifare Ultralight (ISO14443A);
- Mifare Desfire (ISO14443A);
- Mifare Plus (ISO14443A);
- ST SRiX (ISO 14443B).

For other types of cards, contact Iseo to check the compatibility.

CHANNELS mechanism

In the Simply Sequence system, the user’s Credentials are stored in the White List of each access device.

When an USER code or USER card is presented to the reader, the Device checks that the USER Credential is included in its White List and if so, it allows opening the door.

The White List consists of 150 ‘’CHANNELS’’ and each channel can store a sequence of 3 Credentials.

Each sequence of Credentials (CHANNEL) is connected to a single User and vice versa!

Use of the CHANNEL

Up to 3 USER Credentials can be stored in each channel of the White List.

These are all connected to a single user.

The Credential to submit to the user to allow opening the door is stored in the first position of the channel.

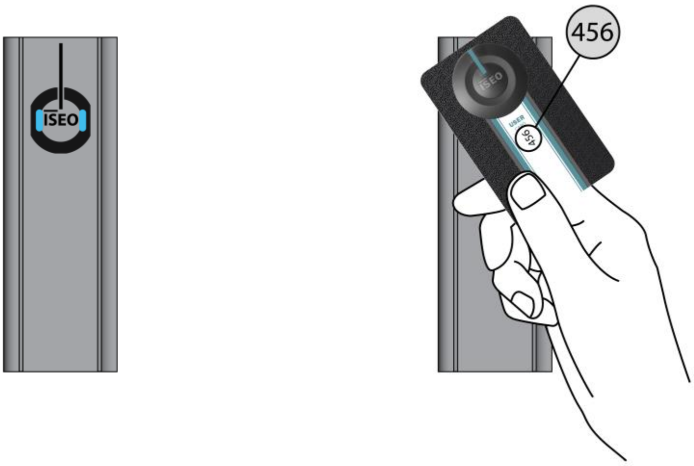
The back-up USER Credentials are stored in the second and third position to disable the first Credential in case this is lost or stolen.

Sequence operation in a CHANNEL

There are two methods to disable a lost USER Credential stored in the first position of the channel:

1) Open the door with the USER Credential stored in the second or third position of the channel. The USER Credentials stored in the same channel in previous positions will be automatically disabled (the use of the USER Credential in third position disables both USER Credentials in first and second position).
2) Delete all the channel’s Credentials using one of the other USER Credentials stored in the same channel, together with the MASTER card

Deleting a lost USER Credential



CHANNEL	ID #1	ID #2	ID #3
1	123	456	789

CHANNEL	ID #1	ID #2	ID #3
1	🚫 123	456	789

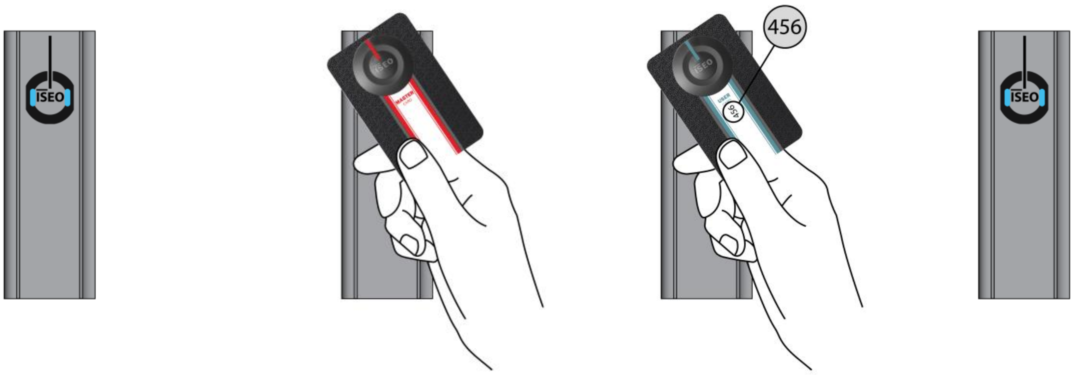
Credential #1 (card 123) is no longer enabled to open the door.

! The reading of Credential #3 disables Credentials #1 and #2 automatically.

Deleting a CHANNEL

In order to completely delete a channel and all USER cards contained in it, bring closer the MASTER card twice and then any USER card of the channel to delete.

The USER cards deleted from a device remain anyhow active in the other devices where they have been stored and they can be re-used.



CHANNEL	ID #1	ID #2	ID #3
1	123	456	789

2 x

1 x

CHANNEL	ID #1	ID #2	ID #3
1			

Elaboration of the Keyplan and storage of the user's Credentials

The user's Credentials can be configured on the device with different functions according to the type of door to monitor.
The special Credentials requested during the storage phase are:

- Very Important People V.I.P.+ Credential, it creates a privileged type of USER card able to configure the door, only to be accessed with V.I.P. cards
- Very Important People V.I.P. Credential, it creates a privileged type of USER card able to open the door, configured only to be accessed with V.I.P. cards
- Toggle Credentials, it creates an additional function for the card that allows enabling the office function.

See chapter *Special Credentials* for the operation of the V.I.P., V.I.P.+ and TOGGLE functions.

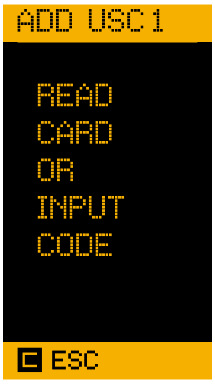
Note down the Credentials using the *Keyplan* enclosed in this manual.

Each device can store up to maximum 150 channels.

Storage of the USER Credentials (PAD ACD)

This procedure allows adding up to three USER Credentials (card or code) to a channel of the device. The Credentials are added to the White List.
Each device can store up to maximum 150 channels with maximum three USER Credentials each.

Sequence:

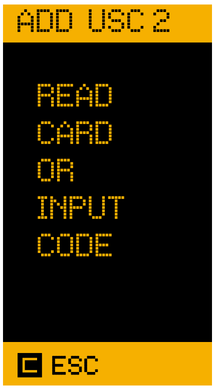


ADD USC 1

READ
CARD
OR
INPUT
CODE

ESC

#1, or numeric code from 4 to 8 digits followed by ↵

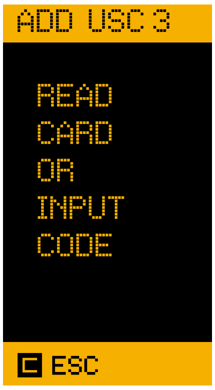


ADD USC 2

READ
CARD
OR
INPUT
CODE

ESC

#2, or numeric code from 4 to 8 digits followed by ↵

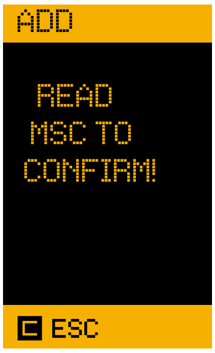


ADD USC 3

READ
CARD
OR
INPUT
CODE

ESC

#3, or numeric code from 4 to 8 digits followed by ↵



ADD

READ
MSC TO
CONFIRM!

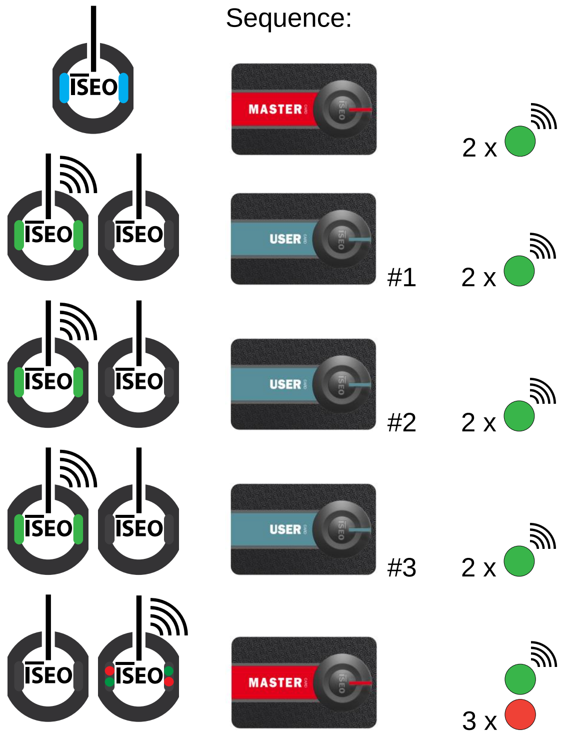
ESC

the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER cards (STANDARD ACD)

This procedure allows adding from one to three USER Cards to a channel of the device.
The Credential is added to the White List. Each device can store up to maximum 150 USER channels. To store more channels, repeat the full procedure more times.

Sequence:



the sequence can be ended the same way after inputting card #1 or card #2

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

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 SEQUENCE - System Keyplan

					Access Control Devices																													
Seq.	Card_ID #1	Card_ID #2	Card_ID #3	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	456	789	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.

USER cards "456" and "789" have been filed in a safe place and will be submitted to user Mario in case of cards "123" or "456" are lost, respectively. Opening the door with higher Card ID disables the Credentials with lower Card ID:

Card_ID #2 disables Card_ID #1

Card_ID #3 disables Card_ID #2 and Card_ID #1

The ID number corresponds to the storage sequence described in the relative PAD ACD and STANDARD ACD chapters.

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

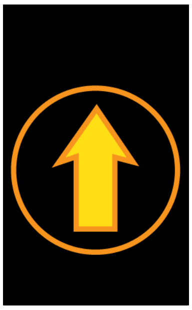
"**V+**" = card with V.I.P.+ function

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

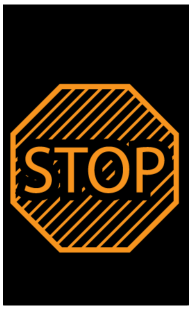
"**TV+**" = card with TOGGLE and V.I.P.+ functions

How to use a Credential to open a door

Opening signals (PAD ACD)



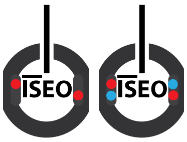
Open door, the actuator have opened it.
The picture blinks during the opening time



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 (Aries 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.

Blocking the door due to wrong code (PAD ACD)

The PAD ACD device can be accessed through code input from keyboard, if stored in the White List.

The inputting of three consecutive wrong codes blocks the device for 1 minute. After this block time, the door can be opened. The inputting of an additional wrong code blocks the door again for 1 minute, further slowing down possible opening attempts from non-authorised users.

The device can be released during the block time through the USER card or a MASTER card.

The restoring through valid card or opening through correct Credential restores the opening attempts prior to the block, to 3.

3 x

Blocked door, wait 1 minute or use

to release it

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 channel in the White List of a device;
- DELETE an USER channel in the White List of a device;
- DELETE all the USER channel in the White List of a device.

The changes to the Keyplan must always be recorded.

USER card Credentials and numeric Credentials are allowed in the PAD ACD device, while only USER card Credentials are allowed in the STANDARD ACD device.

A single channel can be deleted only through one of the USER Credentials present in it.

In case of loss of USER #1 and USER #2 Credentials of a channel, we suggest to use the USER #3 Credential to delete the same channel, and then re-create a new channel consisting of 3 Credentials.
This will avoid to completely delete the channels of the device in case of loss of USER #3 Credential.

Inputting a new CHANNEL (PAD ACD)

The procedure is the same as that used to initially create the CHANNEL.

See chapter "*Storage of USER Credentials (PAD ACD)*"

Inputting a new CHANNEL (STANDARD ACD)

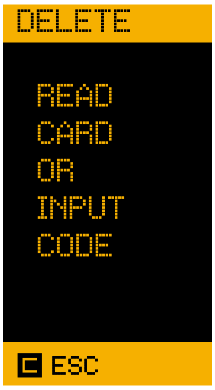
The procedure is the same as that used to initially create the CHANNEL.

See chapter "*Storage of USER Credentials (STANDARD ACD)*"

Deleting a CHANNEL (PAD ACD)

The procedure deletes a channel and all USER Credentials contained in it from the device's White List.
The channel can be deleted only through any Credential stored in it.

Sequence:



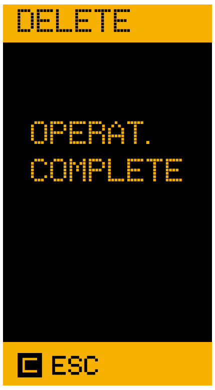
DELETE

READ
CARD
OR
INPUT
CODE

ESC

2 x

, or numeric code from 4 to 8 digits followed by ↵, stored in the channel to delete



DELETE

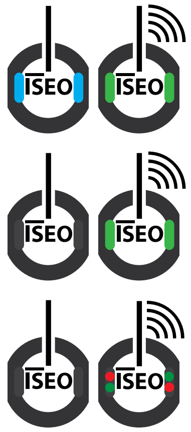
OPERAT.
COMPLETE

ESC

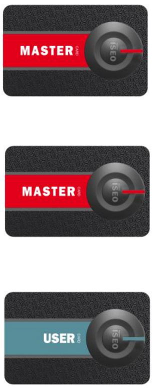
Deletion of channel completed.

Deleting a CHANNEL (STANDARD ACD)

The procedure deletes a channel and all USER Credentials contained in it from the device’s White List. The channel can be deleted only through any USER card stored in it.



Sequence:



2 x 📶🟢

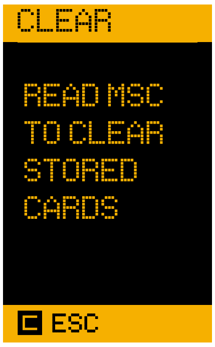
4 x 📶🟢

📶🟢

3 x 🔴

Deleting all the channels and clearing the White List (PAD ACD)

The procedure deletes all channels of the device, emptying the White List.



CLEAR

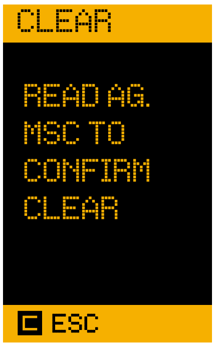
READ MSC
TO CLEAR
STORED
CARDS

ESC

Sequence:

hold the card for over 5 seconds + 2 x 📶

6 x 📶



CLEAR

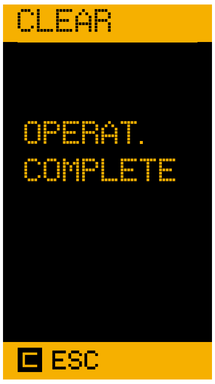
READ AG.
MSC TO
CONFIRM
CLEAR

ESC

hold the card for over 5 seconds + 2 x 📶

6 x 📶

hold the card for over 5 seconds + 2 x 📶



CLEAR

OPERAT.
COMPLETE

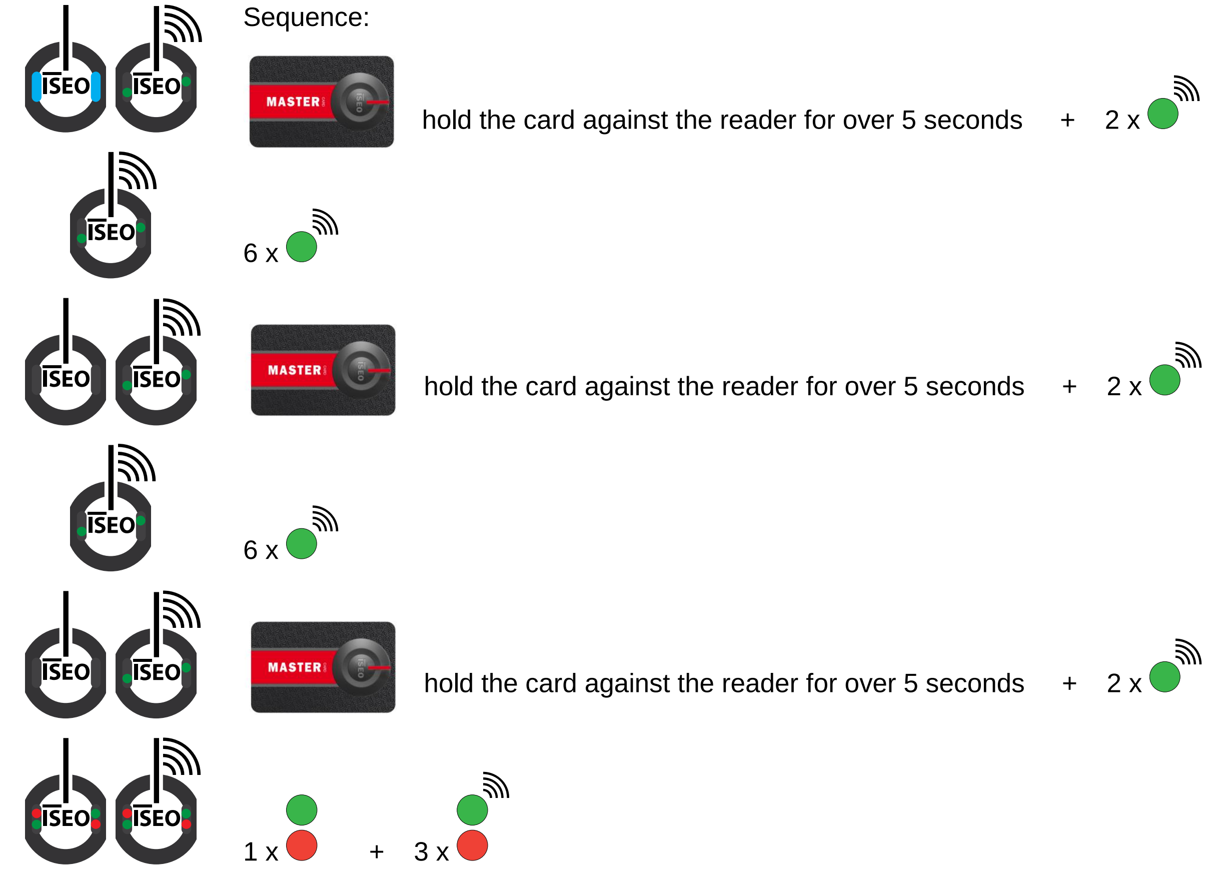
ESC

3 x 📶

device cleared.

Deleting all the channels and clearing the White List (STANDARD ACD)

The procedure deletes all channels of the device, emptying the White List.



Sequence:

MASTER hold the card against the reader for over 5 seconds + 2 x 🟢

6 x 🟢

MASTER hold the card against the reader for over 5 seconds + 2 x 🟢

6 x 🟢

MASTER hold the card against the reader for over 5 seconds + 2 x 🟢

1 x 🟢🔴 + 3 x 🟢🔴

Updating a lost or stolen card

If a USER #1 Credential is lost or stolen, the steps below must be followed:

- submit USER #2 Credential of the same channel to the user
- disable immediately the old USER #1 Credential in all relative devices, opening the door at least once with the newly submitted USER #2 Credential.

If also the USER #2 card is lost or stolen, the steps below must be followed:

- delete the channel assigned to the lost Credential from all relative devices, performing the deletion procedure of the channel with the MASTER card and USER #3 Credential
- input a new channel in all relative devices, assigning new USER #1, #2 and #3 Credentials (#3 Credential of the deleted channel can be re-used)
- submit USER #1 Credential of the newly created channel to the user
- file #2 and #3 Credentials in a safe place.

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:

Hold the card against the reader for at least 3 seconds

or access code + ↵ + ① within 2 seconds.

The door remains opened until the closing sequence.

If the USER Card with TOGGLE Credentials is brought near the standard device for at least 3 seconds, the door opens in normal mode, *for the set opening time*.

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

Closing sequence:

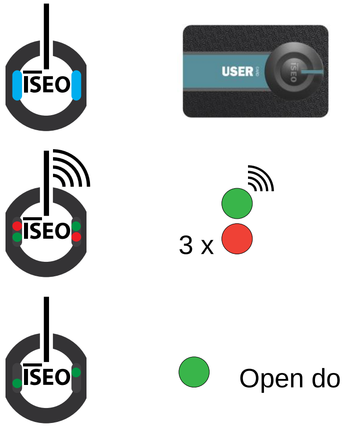
Hold the card against the reader for at least 3 seconds

or access code + ↵ + ① within 2 seconds.

The door closes.

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

Opening sequence:



Hold the card against the reader for at least 3 seconds

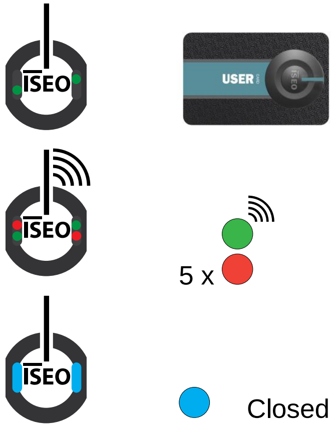
3 x 🟢 🔴

🟢 Open door

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 set opening time.

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

Closing sequence:



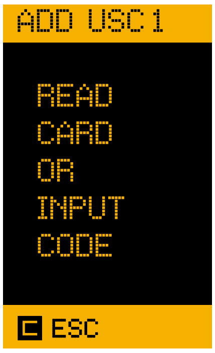
Hold the card against the reader for at least 3 seconds

5 x 🟢 🔴

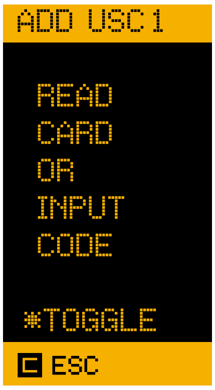
🔵 Closed door

Storage of the USER Credentials with TOGGLE mode (PAD ACD)

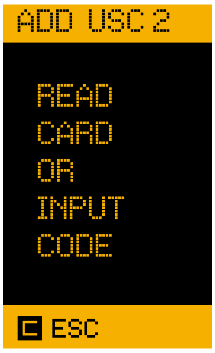
This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active TOGGLE function.


ADD USC 1
READ
CARD
OR
INPUT
CODE
ESC

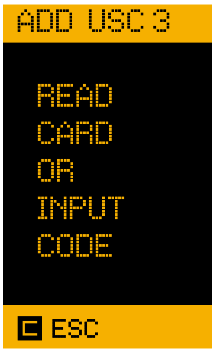
Sequence:


ADD USC 1
READ
CARD
OR
INPUT
CODE
*TOGGLE
ESC

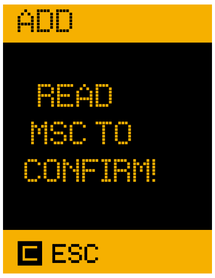
#1, or numeric code from 4 to 8 digits followed by ↵


ADD USC 2
READ
CARD
OR
INPUT
CODE
ESC

#2, or numeric code from 4 to 8 digits followed by ↵


ADD USC 3
READ
CARD
OR
INPUT
CODE
ESC

#3, or numeric code from 4 to 8 digits followed by ↵

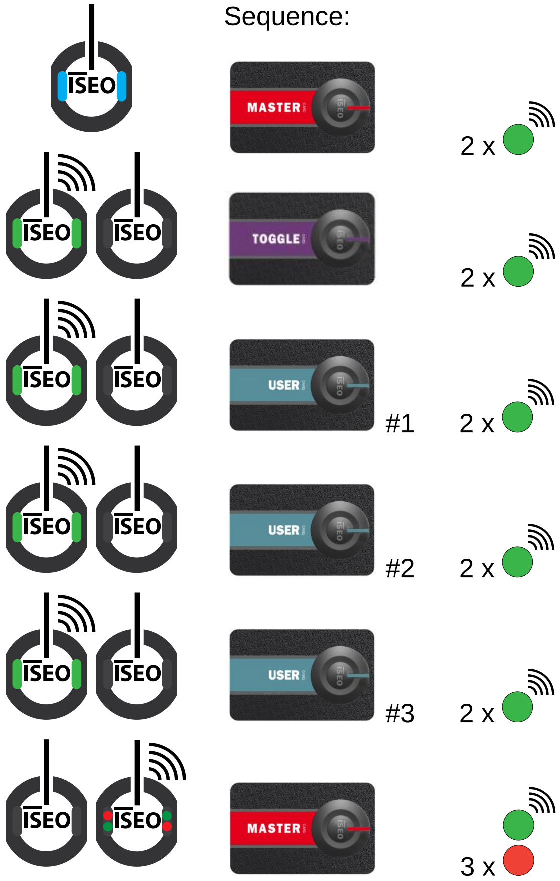

ADD
READ
MSC TO
CONFIRM!
ESC

the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER cards with TOGGLE mode (STANDARD ACD)

This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active TOGGLE function.

Sequence:



the sequence can be ended the same way, after inputting card #1 or card #2

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:
bring closer the USER card 3 times within 6 seconds

3 x

CARD WITH V.I.P.+ MODE ENABLED

or access code + ↵ + 2 within 2 seconds.

The door can be opened only with USER cards with active V.I.P. function

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

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

Deactivation sequence:
bring closer the USER card 3 times within 6 seconds

3 x

CARD WITH V.I.P.+ MODE ENABLED

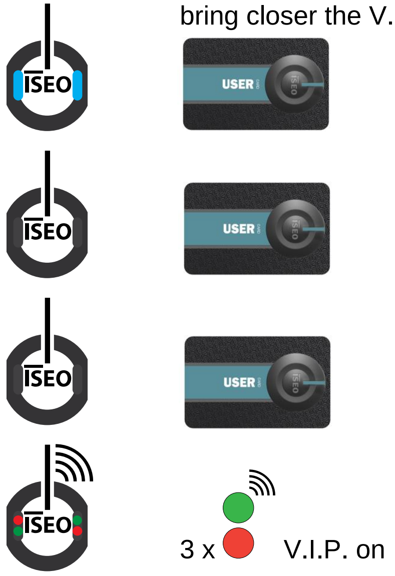
or access code + ↵ + 2 within 2 seconds.

The door can be opened again with all stored USER cards.

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. mode – Very Important People (STANDARD ACD)

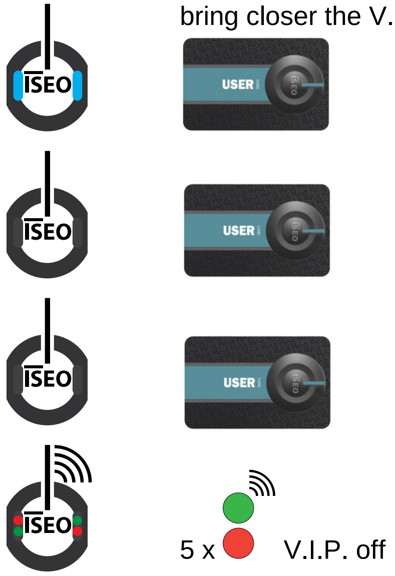
Activation sequence:
bring closer the V.I.P.+ Card 3 times within 6 seconds



If the USER Card with V.I.P.+ function active is brought closer to the device once, the door remains in the same mode and opens for the *opening time*.

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

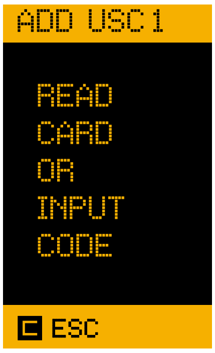
Deactivation sequence:
bring closer the V.I.P.+ Card 3 times within 6 seconds



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

Storage of the USER Credentials with V.I.P. mode (PAD ACD)

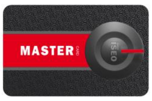
This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active VIP function.

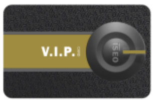

ADD USC1

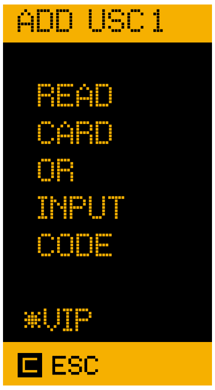
READ
CARD
OR
INPUT
CODE

ESC

Sequence:



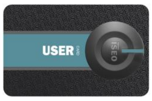



ADD USC1

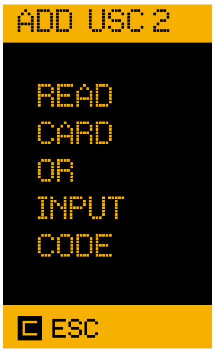
READ
CARD
OR
INPUT
CODE

*VIP

ESC

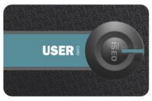


#1, or numeric code from 4 to 8 digits followed by ↵

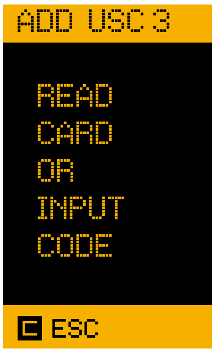

ADD USC2

READ
CARD
OR
INPUT
CODE

ESC

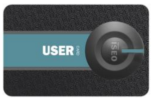


#2, or numeric code from 4 to 8 digits followed by ↵

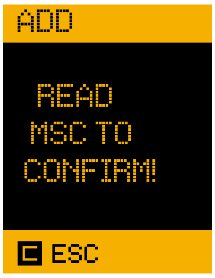

ADD USC3

READ
CARD
OR
INPUT
CODE

ESC

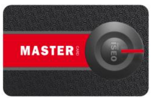


#3, or numeric code from 4 to 8 digits followed by ↵


ADD

READ
MSC TO
CONFIRM!

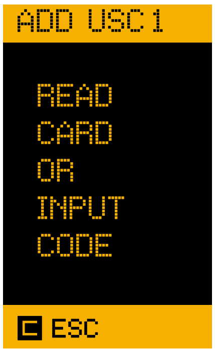
ESC



the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER Credentials with V.I.P.+ mode (PAD ACD)

This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active V.I.P.+ function.

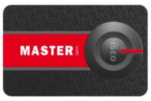


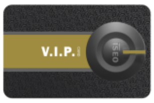
ADD USC 1

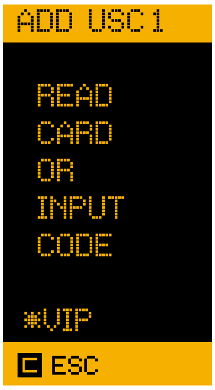
READ
CARD
OR
INPUT
CODE

ESC

Sequence:



2 x 



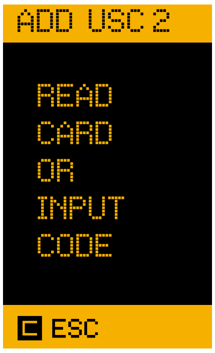
ADD USC 1

READ
CARD
OR
INPUT
CODE

*VIP

ESC

#1, or numeric code from 4 to 8 digits followed by ↵

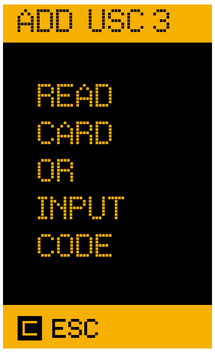


ADD USC 2

READ
CARD
OR
INPUT
CODE

ESC

#2, or numeric code from 4 to 8 digits followed by ↵

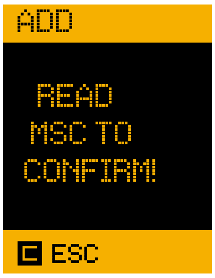


ADD USC 3

READ
CARD
OR
INPUT
CODE

ESC

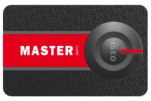
#3, or numeric code from 4 to 8 digits followed by ↵



ADD

READ
MSC TO
CONFIRM!

ESC

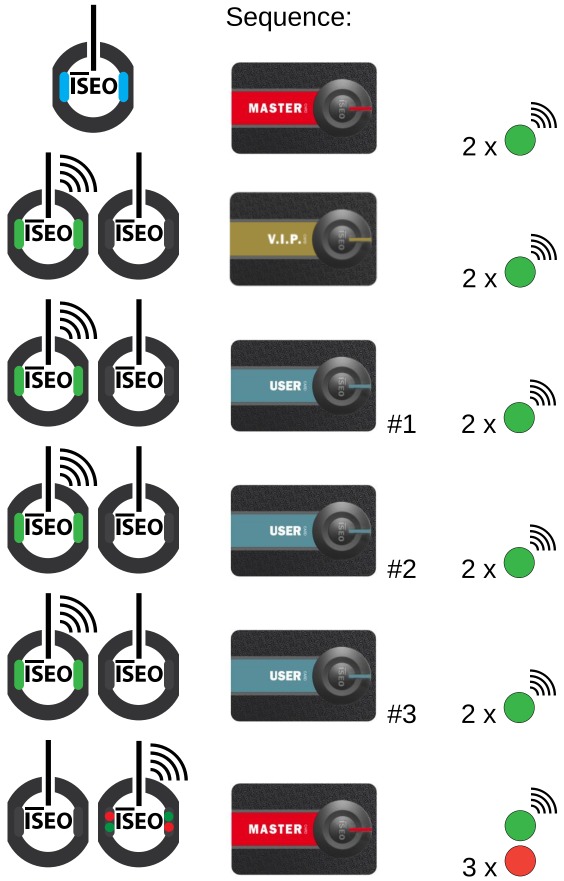


the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER Cards with V.I.P. mode (STANDARD ACD)

This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active VIP function.
The channel is added to the White List.

Sequence:

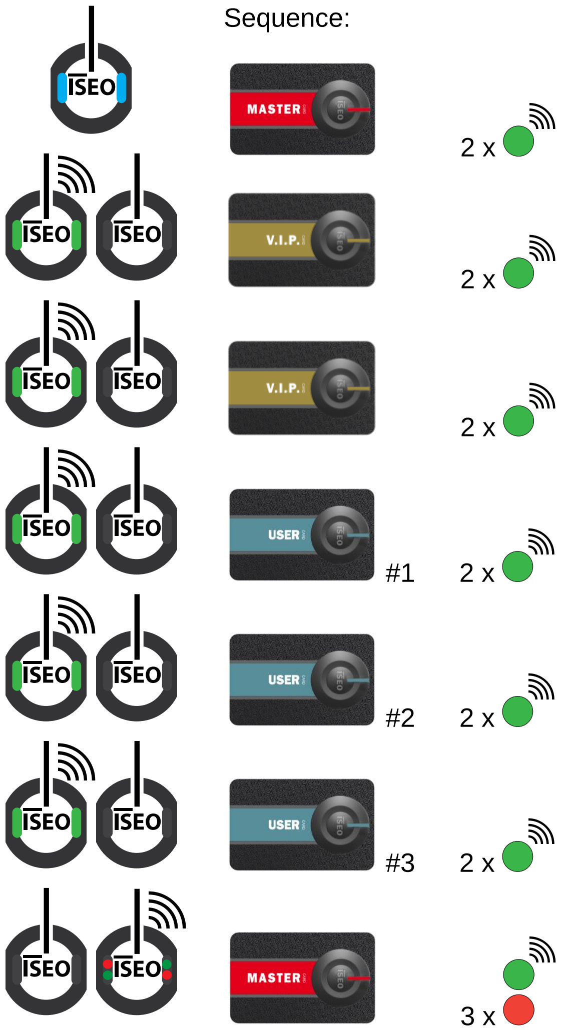


the sequence can be ended the same way after inputting card #1 or card #2

Storage of the USER Cards with V.I.P.+ mode (STANDARD ACD)

This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active V.I.P.+ function.
The channel is added to the White List.

Sequence:

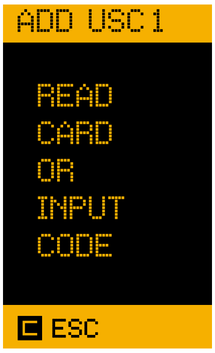


the sequence can be ended the same way after inputting card #1 or card #2

Storage of the USER Credentials with TOGGLE and V.I.P. modes(PAD ACD)

This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active TOGGLE and V.I.P. function.

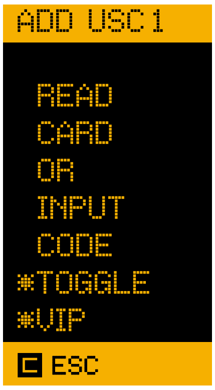
Sequence:



ADD USC1

READ
CARD
OR
INPUT
CODE

ESC

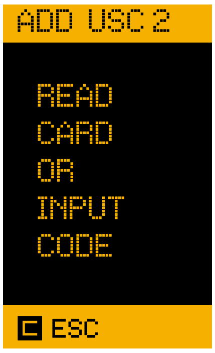


ADD USC1

READ
CARD
OR
INPUT
CODE
*TOGGLE
*VIP

ESC

#1, or numeric code from 4 to 8 digits followed by ↵

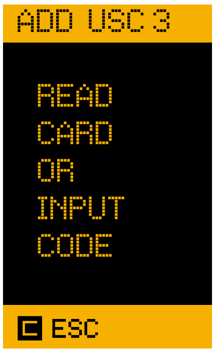


ADD USC2

READ
CARD
OR
INPUT
CODE

ESC

#2, or numeric code from 4 to 8 digits followed by ↵

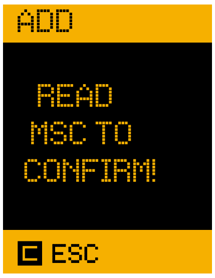


ADD USC3

READ
CARD
OR
INPUT
CODE

ESC

#3, or numeric code from 4 to 8 digits followed by ↵



ADD

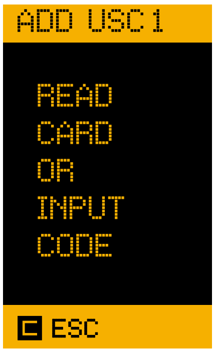
READ
MSC TO
CONFIRM!

ESC

the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER Credentials with TOGGLE and V.I.P.+ modes(PAD ACD)

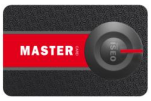
This procedure allows adding three USER Credentials (card or code) to a channel of the device, with active TOGGLE and V.I.P.+ function.

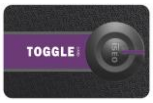

ADD USC 1

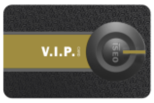
READ
CARD
OR
INPUT
CODE

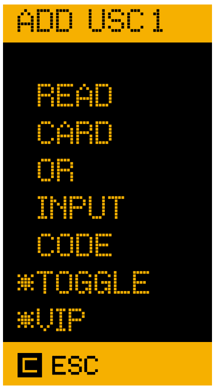
ESC

Sequence:



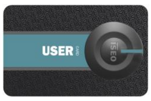


2 x 

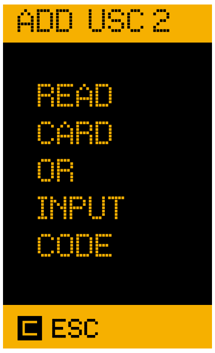

ADD USC 1

READ
CARD
OR
INPUT
CODE
*TOGGLE
*VIP

ESC

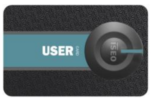


#1, or numeric code from 4 to 8 digits followed by ↵

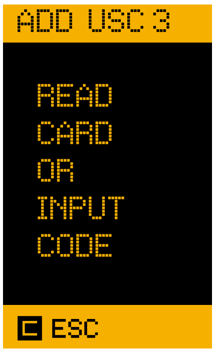

ADD USC 2

READ
CARD
OR
INPUT
CODE

ESC

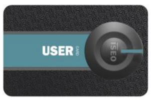


#2, or numeric code from 4 to 8 digits followed by ↵

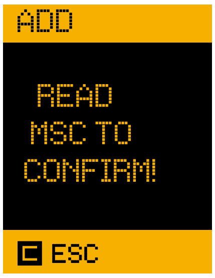

ADD USC 3

READ
CARD
OR
INPUT
CODE

ESC

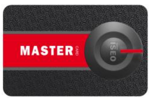


#3, or numeric code from 4 to 8 digits followed by ↵


ADD

READ
MSC TO
CONFIRM!

ESC

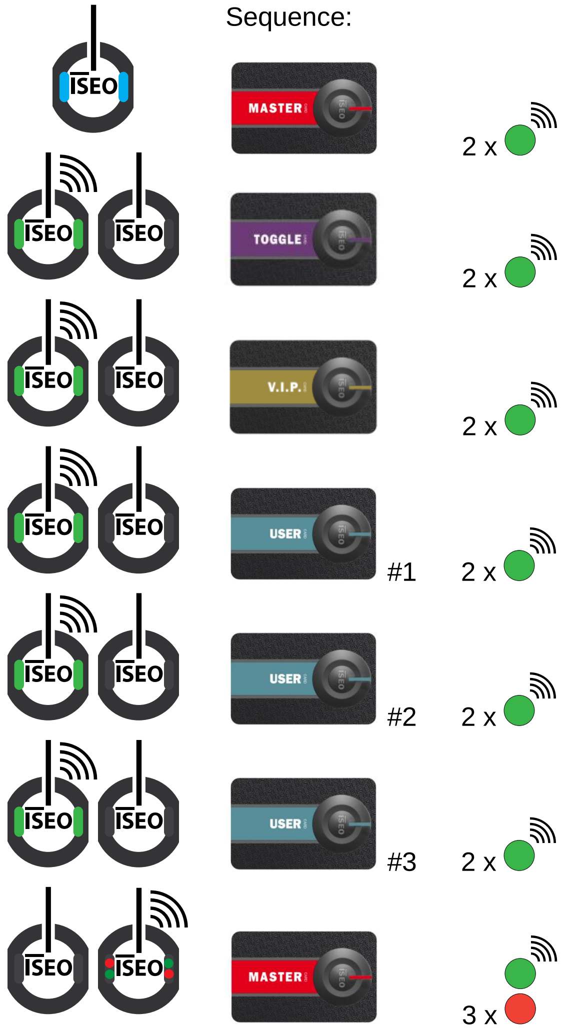


the sequence can be ended the same way after inputting Credential #1 or Credential #2

Storage of the USER Cards with TOGGLE and V.I.P. modes (STANDARD ACD)

This procedure allows adding three USER Credentials to a channel of the device, with active TOGGLE and V.I.P. function.
The channel is added to the White List.

Sequence:

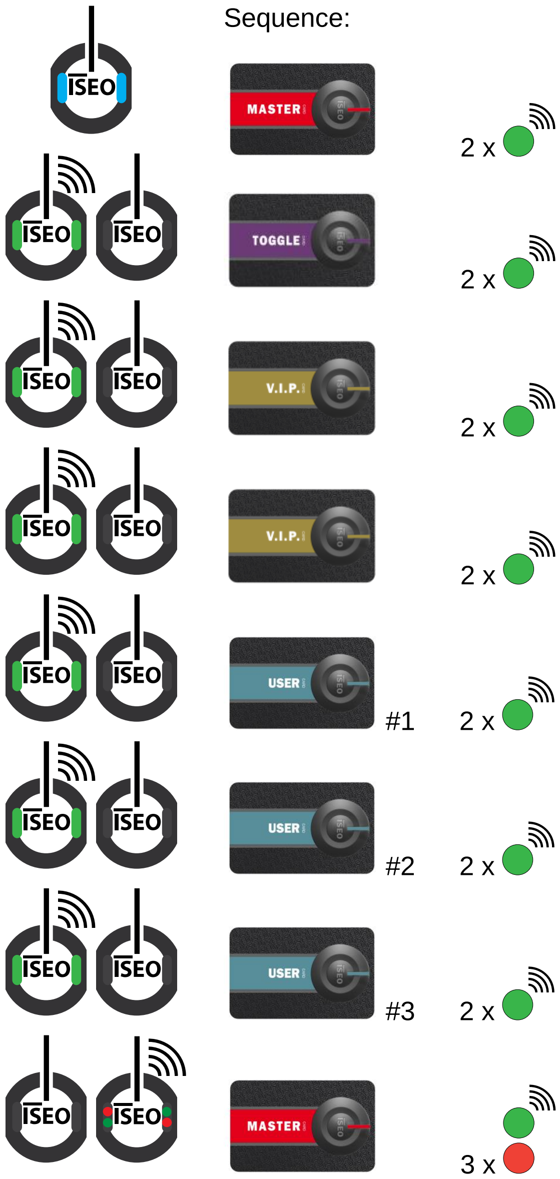


the sequence can be ended the same way after inputting card #1 or card #2

Storage of the USER Cards with TOGGLE and V.I.P.+ modes (STANDARD ACD)

This procedure allows adding three USER Credentials to a channel of the device, with active TOGGLE and V.I.P.+ function.
The channel is added to the White List.

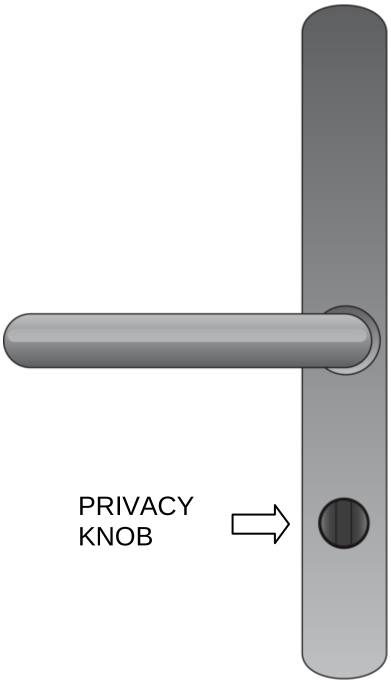
Sequence:

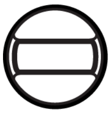


the sequence can be ended the same way after inputting card #1 or card #2

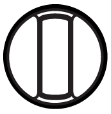
PRIVACY mode (only for the ELECTRONIC TRIM device)

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.





Enabled PRIVACY mode

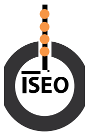


Disabled PRIVACY mode

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.

or



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.

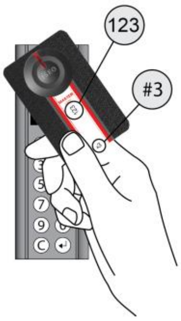
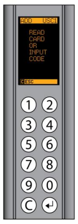
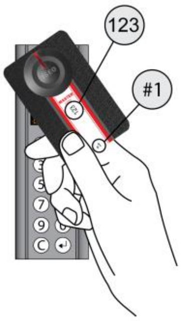
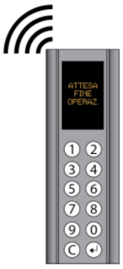
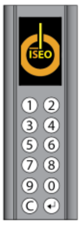
- By bringing MASTER card #2 closer to the device, MASTER card #1 is disabled.
- By bringing MASTER card #3 closer to the device, MASTER cards #2 and #1 are disabled.

WARNING

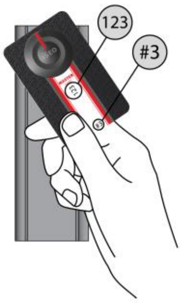
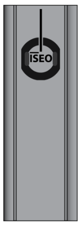
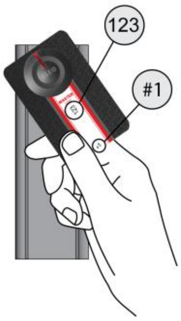
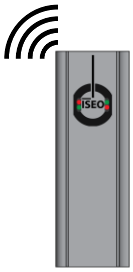
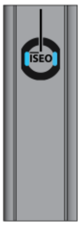
Authenticate the MASTER card of higher number only if the card of lower number has been lost or stolen, since the authentication of a MASTER card will disable the MASTER cards of lower number.

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 #1 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

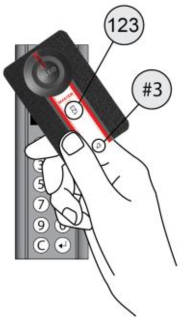
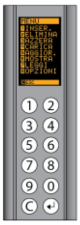
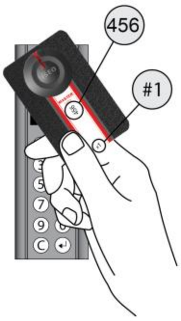
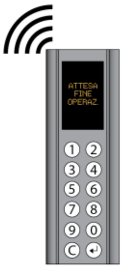
If both MASTER cards #1 and #2 are lost, in order to ensure the system's security, you must update the system's devices with a new SET of MASTER credentials (**if MASTER card #3 is lost, it will not be longer possible to operate on the system's devices).**

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.

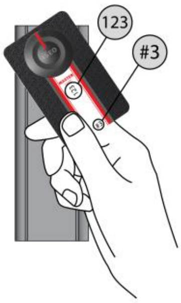
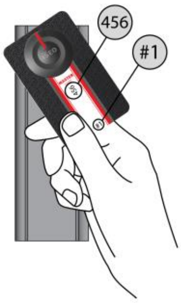
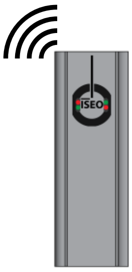
No change is made to the User’s List of the devices.

! 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
	 MENU INSER. ELIMINA AZZERA CARICA AGGIOR. MOSTRA LEGGI OPZIONI			

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 SEQUENCE - System Keyplan

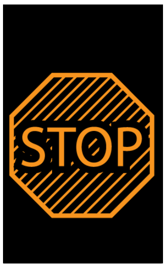
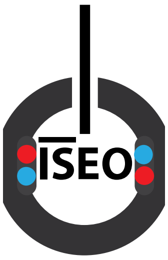
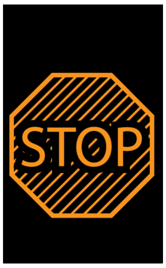
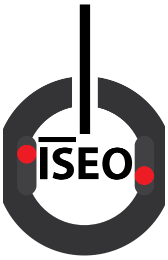
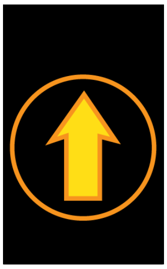
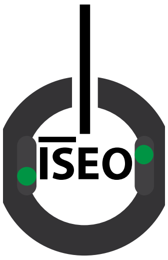
					Access Control Devices																													
Seq.	Card_ID #1	Card_ID #2	Card_ID #3	User Name	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	#18	#19	#20	#21	#22	#23	#24	#25	#26	#27	#28	#29	#30
1																																		
2																																		
3																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

Glossary

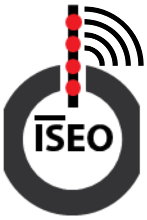
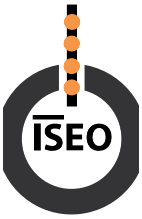
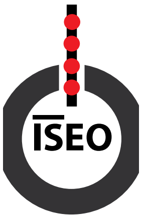
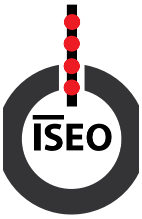
Access Control:	system of electronic and/or mechanical devices to allow selective access through the users' doors.
Door:	passage or door which access is electronically controlled by the ACD (access control devices).
Credential:	device that allows to identify the user and authorise or non-authorise access 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.
Channel:	the series consisting of up to three Credentials assigned to a single USER stored in the White List
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.
Timeout:	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

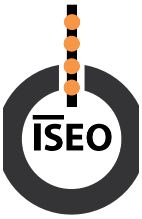
Common for all the devices

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.

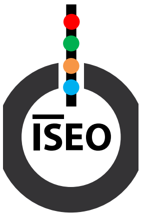
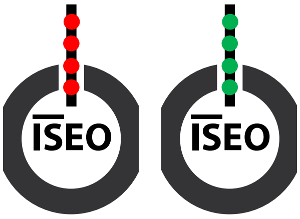
Signals following the change of battery

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

60000SSEPDF01 –05/02/2014 – Documento non contrattuale. Con riserva di modifica.

ISEO Zero1
ELECTRONIC SUPPORT SERVICE
iseozero1@iseo.com