# ARGO access control system

**The solution includes the following products:**

- ARGO APP

**Specification:**

ISEO ARGO access control system with BT 4.0 embedded interface, compatible with the Iseo ARGO App on Bluetooth Smart Ready devices such as smartphones and tablets, to program and manage the access control criteria. The Argo APP must be available for iOS and Android and allow to add new opening devices like cards, tags or phones, retrieve events logs, delete lost/stolen cards or smartphones, send key remotely and update the access control systems to new software features. The Argo system must be available on Libra SMART electronic cylinder, on Aries SMART electronic trim, Stylos SMART readers and X1R SMART locks for armoured doors. The SMART access control devices must be opened by RFID cards and Bluetooth Smart Ready phones (iOS and Android). Lost or stolen keys must be quickly deleted with Argo, an intuitive smartphone application available for iOS from iOS 10 or Android from version 5.0 (Lollipop) featuring Bluetooth smart ready hardware. The system must have 3 levels MASTER cards set, keeping a safe system management even in case of lost MASTER cards, operate with Iseo card or Legacy Mifare cards (contactless credit cards, public transportation tickets, time attendance cards…), memorize up to 300 users (cards or phones), record the last 1000 events and be able to start and end validity date for each user management qnd weekdays time tables access for each user management (up to 2 time tables per user), door schedules, invitations and Remote Key Delivery, remote opening and communication with Bluetooth Smart ready phone up to 10 meters, software upgradable on site via the Bluetooth Smart Ready phone. The Argo App must allow the user to open doors as well to easily manage access authorizations. There must not be any additional software to install and must work even if it is not connected to Internet as the Argo App must connect directly to the doorlock with the latest encryption protocols ensuring the highest security in data transfers. The users must be able to open doors with smartphone from remote up to 10 meters with smartphone protected with PIN code, with cards or tags and with PIN code (only devices with keypad). In addition it must be possible to temporarily block the standard users allowing access only to VIP users, set the door in passage mode (office mode), get early notification of low battery or availability of new software for the Libra Smart. Administrators manage access authorizations to doors adding new users (cards, tags, PIN codes or smartphones), removing users, transferring user lists to other doors, read door events and track users passages, read Smart devices status, add doorlock new feature with easy Software upgrade from the App store or Google Play. The battery level icon must be always displayed on the Argo app button corresponding to the specific lock.

The battery status must be visible when opening the door with specific light signals on the Smart lock. There must be 4 battery charge levels to see in advance when the battery needs to be replaced. Battery replacement must not delete the user list or the events log. The Argo app must work without the Internet as it connects to the lock directly via Bluetooth Smart, ensuring the highest security with encrypted communication. Argo must guarantee data confidentiality and authentication with proven cryptography techniques based on Crypto AES 128, AES session keys generated with DHEC (Diffie Hellman Elliptic Curves) and random Number generator complying with NIST (National Institute of Standards and Technology). The time control must be used to set the validity of the assigned credential (date and time of activation and expiry) for each user, as well as two time schedules that must be selected for each day of the week. It must be also possible to set merely the validity from the moment of the first use of the credential (in days, hours or minutes). The validity from the first use must be combined with the activation and expiry date, and with the time schedules of the credential. The system must allow smartphones to self-register in the locks as users through the invitation function. This function must allow users to add their smartphone to the user list thanks to the invitation code, without needing to physically take the smartphone near to the door for data storage purposes. The administrator must first of all programme the invitation code on the lock as one of the 300 users. When the user arrives in front of the door, he/she must select it and type in the invitation code. The door is opened via the smartphone. At the same time, the telephone must self-register in the user list for the period of time specified in the invitation. The invitation code must be used once only. The remote Key Delivery function on locks of the Smart range must permit to give the users the possibility of remote access manage remotely through the Argo Cloud platform available for the Argo remote virtual key delivery service).