Cidron white paper

General reader information & applications

Cidron readers provide multiple platforms of RFID technologies and communication interfaces equipped with an LED bar and a mechanical keypad in a timeless design. Cidron readers suites almost all kind of applications and environments for indoor and outdoor use. Common applications include: industrial buildings, military installations, education establishments, healthcare buildings, commercial buildings, government buildings. Installations can be from a lower up to the highest level of security.

Cidron readers incorporate several chip technologies and communication interface standards. For access control systems supporting OSDP secure channel, a credential transaction can be complete AES 128 encrypted secured during the card reading and transmitting process between the reader and the access control controller.

In addition to traditional radio frequency technologies such as 13,56MHz and 125KHz also BLE, NFC and SAM AV2 are supported. This combination makes the product flexible for all kinds of security applications and future technology requirements applicable to the security industry.

The LED bar indicates in combination with a buzzer sounds a user-friendly and clear information in real-time for the user.

Cidron readers are tamper protected with a mechanical switch which allows for indication both on attempts to break off and manipulation of the reader.

Production, Design & assembling

Cidron products are specified and designed to meet requirements specified and requested from the European and US security market. All the product design is made in Sweden. The combination to integrate experience from the security business with industrial design knowledge and the latest within the RFID technology has created a product that can be installed in almost all different environmental applications. As well as meet all function and feature requirements from the market. It has also allowed providing a flexible product that is cost-effective to produce, can be partly assembled before delivery and is easy to install.

This combination ensures that the product design can meet the environmental requirements related to weather conditions, usability and performance for high-security applications.

Approvals and compliance

CE 2011/65/EU, CE 2015/863/EU, RoHS3, RED 2014/EU, US FCC part 15.

RF frequencies

13,56MHz, 125KHz, 2,4GHz

ISO standards

ISO14443A/B, ISO18092 & ISO7816

Card technologies

Contactless smart cards are the most becoming technology of choice for access control applications. Security, convenience and interoperability are the three major reasons for this growth. Since there is a wide variety of reader technologies being offered by today's manufacturers, it is important to make sure that the correct technology is chosen to match the desired level of security. Readers that provide several standard card technologies secure the level of security for the future.

Cidron readers support a wide spectra of ISO standard card technologies. ISO standards provided is ISO 14443A/B containing Mifare Classic sector & UID 4 & 7Byte, Mifare Desfire EV1, EV2 and CSN, Mifare plus sector & UID, Mifare Random UID and iClass UID. Cidron combi reader model equipped with Dual antennas due also support 125kHzcard technologies such as HID Prox, and Elektro Marine (EM 4100, 4102).

SL v.20-041.0

Seriline AB Gustavslundsvägen 50, 167 51 Bromma | Sweden +46 (0) 10 - 150 75 00 info@seriline.com www.seriline.com

Communication Interfacing technologies & standard protocol

OSDP, OSDP Secure Channel, RS485, Weigand, Clock/Data, Bluetooth BLE, NFC.

Software & data storage

Cidron readers can be programmed and configured from an associated PC software connected in serial to the reader device or by a configuration card which requires an authorization card permission to set the reader in a programable mode. The PC software, Cidron reader tool, is developed and maintained in Sweden. The Cidron reader tool requires a username and a password to login to the software. It is not possible to read any configuration from the card reader. Encryption keys can be hidden in the configuration and cannot be recreated in the Cidron reader tool or any other software.

If using configuration cards, you first need to use a permitted authentication card. When authentication is permitted the reader will be in a configuration mode for 10 seconds and ready to get new settings from the configuration card. After 10 seconds the reader will go back to normal mode again.

All programming cards are using Desfire and AES 128 encryption. Encryption keys can be unique individual for a reader or for a group of readers belonging to a certain site, area or customer etc. All settings and data regarding authentification- and configuration cards are fabricated in Sweden.

Custom unique data such as encryption keys can be stored in the reader memory chip or on a SAM AV2 SIM card located in the reader. The internal reader MCU memory has a read-out lock to protect against hacking or manipulation attempts on the product. The SAM AV2 module SIM card is equipped with an EAL5+ security data protection level.

During the production process of the reader, an embedded version of the firmware is installed to be able to complete tests in the manufacturing procedures. The readers contain this firmware when they arrive at Serilines warehouse in Sweden.

When a reader is assembled at Seriline in Stockholm, the readers will be given the correct firmware and configuration, with programmable data settings. This is executed with the Cidron reader tool. Depending on the request, all configuration settings can be done by Seriline, integrator/installer or end-customer and can be downloaded to the reader from a configuration card when the reader is installed on-site.

Connection availability

A Cidron reader can only perform and act together as a reader device, connected to an access control system controller. The reader is 100% transparent and has no intelligence to make decisions about granted or denied access after a card is presented and read by the reader. Neither to transmit commands to any other external system such as arm/disarm commands to an intrusion alarm system etc. A Cidron reader can only act on an order from the access control system that host the reader. Either which communication interface that is used between a Cidron online reader or a controller, all decisions and behavior are requested from the access control system controller.

If the reader is out for manipulation, is removed or disassembled from the wall, the reader will enter a tamper alarm mode. The Cidron online reader does not contain any parts that can be manipulated to open a door and can, therefore, be installed in also unsafe and public areas without any security risk.

The Cidron reader does not have an internet connection and can only communicate over the communication interface controlled by the access control system controller. There is no other possible way to communicate with a Cidron reader.

Cidron reader product series

Cidron reader product series contains 13 different modules as specified as bellow with the model number.

SC9100-MD	Cidron reader Standard 13,56MHz with keypad
SC9110-MD	Cidron reader Standard 13,56MHz without keypad
SC9100-MDE	Cidron reader Combi 13,56MHz/125kHz with keypad
SC9110-MDE	Cidron reader Combi 13,56MHz/125kHz without keypad
SC9200-MD	Cidron reader Slimline 13,56MHz with keypad
SC9210-MD	Cidron reader Slimline 13,56MHz without keypad
SC9230-MD	Cidron E reader Slimline 13,56MHz without keypad
SC93100-MDB	Cidron reader VG3 Standard 13,56MHz/BLE with keypad
SC93110-MDB	Cidron reader VG3 Standard 13,56MHz/BLE without keypad
SC93100-MDEB	Cidron reader VG3 Combi 13.56Mhz/125Khz/BLE with keypad
SC93110-MDEB	Cidron reader VG3 Combi 13.56Mhz/125Khz/BLE without keypad
SC93200-MDB	Cidron reader VG3 Slimline 13,56MHz/BLE with keypad
SC93210-MDB	Cidron reader VG3 Slimline 13,56MHz/BLE without keypad

SL v.20-041.0

Seriline AB Gustavslundsvägen 50, 167 51 Bromma | Sweden +46 (0) 10 - 150 75 00 info@seriline.com www.seriline.com