QxControl™ & STiD Architect®Blue

RFID ACCESS CARD & BIOMETRIC READER

MULTI-TECHNOLOGY MIFARE® DESFIRE® EV2 & EV3, NFC AND BLUETOOTH®

The Architect® Blue biometric reader combines the latest RFID MIFARE® DESFire® EV2 & EV3 technologies with digital fingerprint recognition to ensure a strong authentication of the user and enhance the security of your access control system.

HIGHLIGHTS

Features

- Strong multi-factor authentication
- GDPR legislation compliant
- Embedded anti-fraud features
- Interoperable and multi-protocol

EASY FINGERPRINT MANAGEMENT

Different possibilities of fingerprint management depending on your security needs:

- Fingerprint templates directly stored in the RFID card (CNIL French & GDPR European legislation compliance).
- Fingerprint templates stored in the system.
- Card only mode with derogation at the card level (one-time visitor, difficult finger...).
- Smartphone with biometric unlocking or Smartphone only with derogation.

WELCOME TO HIGH SECURITY

RFID MIFARE® DESFire® EV2 & EV3

The reader supports the latest contactless technologies with the newest data security devices:

- Secure Messaging EV2: transaction security that protects against interleaving and replay attacks.
- Proximity Check: protection against relay attacks.

It integrates recognized and approved security mechanisms such as public algorithms and an EAL5+ certified crypto processor to protect your data stored in the reader.

ADVANCED ANTI-FRAUD FUNCTIONS

The Architect® Blue biometric reader is designed to resist fraud attempts:.

False finger detection: the reader detects a wide range of counterfeit fingerprints made of latex, Kapton, transparent film, rubber, graphite, etc.

Detection of live fingers.

Duress finger: the admin can assign a finger number dedicated to authentication when the user is threatened.

ULTIMATE SELF-PROTECTION

The patented motion sensor pull detection system protects sensitive data by allowing authentication keys to be erased.

Unlike existing solutions within this market, the reliability of the accelerometer avoids potential system bypass.

Bluetooth® and NFC smartphones

The smartphone* becomes your access key and erases all the constraints of traditional access control. STid offers 6 identification modes - Prox, long distance or hands-free to make your access control both secure and instinctive.

*The smartphone can be used as a biometric derogation. There is no fingerprint stored in the virtual card.

SPECIFICATIONS

Operating frequency / Standards	13.56 MHz: ISO14443 types A & B, ISO18092 Bluetooth®
Technology compatibilities	MIFARE® Classic & Classic EV1 (4 kb), MIFARE® Plus® (S/X) & Plus® EV1, MIFARE® DESFire® 256 (1 fingerprint), EV1, EV2 & EV3 STid Mobile ID® (NFC and Bluetooth® virtual card), Orange Pack ID
Functions	Read only CSN and secure (file, sector) / Controlled by protocol (read-write)
Digital fingerprint sensor	Optical (SAFRAN MorphoSmart™ CBM E3) - ≤ 1 second for a 1:1 authentication Fingerprint stored in the RFID card or in the system / No fingerprint stored in the virtual card
Communication interfaces & protocols	TTL Data Clock (ISO2) or Wiegand output (encrypted option - S31) / RS485 output (encrypted option - S33) with secure SSCP® v1 and v2 communication protocols, OSDP™ v1 (plain communication) and v2 (SCP secure communication) Compatible with EasySecure interface
Decoder compatibility	Compatible with EasySecure interface (encrypted communication)
Reading distances**	Up to 8 cm / 3.15" with a MIFARE® DESFire® EV2 or EV3 card Up to 20 m / 65.6 ft with a Bluetooth® smartphone (adjustable distances on each reader)
Data protection	Yes - Software protection and EAL5+ crypto processor for secure keys storage
Integrated UHF chip	EPC 1 Gen 2 for contactless reader configuration (protocols, LEDs, buzzer...)
Light indicator	2 RGB LEDs - 360 colors Configurable by card (classic or virtual with STid Settings application), software or controlled by external command (0V) depending on interface
Audio indicator	Internal buzzer with adjustable intensity Configurable by card (classic or virtual with STid Settings application), software or controlled by external command (0V) depending on interface
Relay	Automatic tamper detection management or SSCP® / OSDPTM command according to the interface
Power requirement	Max 300 mA / 12 VDC
Power supply	7 VDC to 28 VDC
Connections	10-pin plug-in connector (5 mm / 0.2") / 2-pin plug-in connector (5 mm / 0.2"): O/C contact - Tamper detection signal
Materials	ABS-PC UL-V0 (black) / ASA-PC-UL-V0 UV (white)
Dimensions (h x w x d)	148.6 x 80 x 71.3 mm / 5.63" x 3.15" x 2.80" (general tolerance following ISO NFT 58-000 standard)
Operating temperatures	- 10°C to + 50°C / + 14°F to + 122°F
Tamper switch	Accelerometer-based tamper detection system with key deletion option (patented solution) and/or message to the controller
Protection / Resistance	IP65 Level - Weather-resistant with waterproof electronics (CEI NF EN 61086 homologation) Humidity: 0 - 95%
Mounting	Compatible with any surfaces and metal walls - Wall mount/Flush mount: -European 60 & 62 mm / 2.36" & 2.44" -American (metal/plastic) - 83.3 mm / 3.27" - Dimensions: 101.6 x 53.8 x 57.15 mm / 3.98" x 2.09" x 2.24" - Examples: Hubbel-Raco 674, Carlon B120A-UP
Certifications	CE (Europe), FCC (USA), IC (Canada), UKCA (United Kingdom) and UL

Part Numbers:

y: color casing (1: black - 2: white)

READ ONLY

Secure - TTL:	**ARCS-R31-D/BT1-xx/y**
Secure / Secure Plus - TTL:	**ARCS-S31-D/BT1-xx/y**
Secure - RS485:	**ARCS-R33-D/BT1-7AB/y**
Secure / EasySecure interface - RS485:	**ARCS-R33-D/BT1-7AA/y**
Secure / Secure Plus - RS485:	**ARCS-S33-D/BT1-7AB/y**
Secure / Secure Plus / EasySecure interface - RS48:	**ARCS-S33-D/BT1-7AA/y**

CONTROLLED BY PROTOCOL

SSCP® v1 - RS485:	**ARCS-W33-D/BT1-7AA/y**
SSCP® v2 - RS485:	**ARCS-W33-D/BT1-7AD/y**
OSDP™ v1 & v2 - RS485:	**ARCS-W33-D/BT1-7OS/y**

**Caution: information about the distance of communication: measured from the center of the antenna, depending on the type of credential, size of the credential, operating environment of the reader, temperatures, power supply voltage and reading functions (secure reading). External interference may reduce reading distances.