QxControl™ & STiD Architect®Blue

UPGRADABLE HIGH SECURITY READER

RFID MIFARE® DESFIRE® EV2 & EV3 CARDS, NFC & BLUETOOTH®

Compatible with all access control systems, Architect® Blue is an vandal-proof reader for RFID cards and Bluetooth® & NFC smartphones.

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.

Display of your logo, images and customized text

HIGHLIGHTS

Features

- RFID, Bluetooth® and NFC secure identification
- Higher levels of security with open technologies
- Modular concept for maximum cost optimization
- Simplified installation with plug-in terminal block
- Interoperable and multi-protocol

WELCOME TO HIGH SECURITY

The reader allows the secure identification of users thanks to its multiple identification technologies.

Bluetooth® and NFC

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!

RFID MIFARE® DESFire® EV2 & EV3

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

- Secure Messaging EV2: protection against attacks via interleaving and replay.
- Proximity Check: protection against relay attacks.

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.

CREATE YOUR OWN SCALABLE CONFIGURATION

The Architect® Blue reader can be tailored to your needs, ensuring that all functionalities and security levels can be upgraded across all your readers - by RFID credential, virtual card or protocol.

The scalability allows you to implement new functionality such as a touch screen/keypad, QR Code or biometric module.

OUR SECURITY OFFERINGS

- **Easyline:** readers and cards pre-configured and programmed, ready to use.
- **•Expert line**: you program your readers and cards in perfect autonomy with the intuitive configuration tools.
- **Individual line**: we offer a wide range of Premium services to configure and customize your readers and credentials according to your needs.

SPECIFICATIONS

Operating frequency / Standards	13.56 MHz: ISO14443 types A & B, ISO18092 Bluetooth®
Chip compatibility	MIFARE® Ultralight® & Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus® (S/X) & Plus® EV1, MIFARE® DESFire® 256, EV1, EV2 & EV3, CPS3, NFC (HCE), PicoPass® (CSN only), iCLASS™ (CSN only*) STid Mobile ID® (NFC and Bluetooth® virtual card), Orange Pack ID
Functions	Read only CSN, pre-configured (Easyline - PC2) and secure (file, sector) / Controlled by protocol (read-write)
Communication interfaces & protocols	TTL Clock & Data (ISO2) or Wiegand output (encrypted communication option - S31) / RS485 outputs (encrypted option - S33) with SSCP® v1 & v2 secure communication protocols; OSDP™ v1 (plain) and v2 (SCP secure)
Decoder compatibility	Compatible with EasySecure interface (encrypted communication)
Reading distances**	Up to 8 cm / 3.15" with a MIFARE® DESFire® EV2 card Up to 20 m / 65.6 ft with a Bluetooth® smartphone (adjustable distances on each reader)
Data protection	Yes - EAL5+ secure data storage with certified crypto processor
Light indicator	2 RGB LEDs - 360 colors Configuration by standard or virtual card with STid Settings application, software or external command (0V) according to the interface
Audio indicator	Internal buzzer with adjustable intensity Configuration by standard or virtual card with STid Settings application, software or external command (0V) according to the interface
Relay	Automatic tamper direction management or SSCP® / OSDPTM command according to the interface
Power requirement	200 mA / 12 VDC Max
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)	106.64 x 80 x 25.70 mm / 4.21" x 3.15" x 1.02" (general tolerance following ISO NFT 58-000 standard)
Operating temperatures	- 30 °C to + 70°C / - 22°F to + 158°F
Tamper switch	Accelerometer-based tamper detection system with key deletion option (patented solution) and/or message to the controller
Protection / Resistance	IP65 Level excluding connector - Weather-resistant with waterproof electronics (CEI NF EN 61086 homologation) Humidity: 0 - 95% / Reinforced vandal-proof structure IK10 certified
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) and UL

Part Numbers:

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

Easyline pre-configured offer - Wiegand:	**ARCS-R31-A/PC2-xx/1**
Secure - TTL Wiegand or Clock & Data:	**ARCS-R31-A/BT1-xx/y**
Secure / Secure Plus - TTL Wiegand or Clock & Data:	**ARCS-S31-A/BT1-xx/y**
Secure - RS485:	**ARCS-R33-A/BT1-7AB/y**
Secure / EasySecure decoder - RS485:	**ARCS-R33-A/BT1-7AA/y**
Secure / Secure Plus - RS485:	**ARCS-S33-A/BT1-7AB/y**
Secure / Secure Plus / EasySecure decoder - RS485:	**ARCS-S33-A/BT1-7AA/y**
Controlled by SSCP® v1 protocol - RS485:	**ARCS-W33-A/BT1-7AA/y**
Controlled by SSCP® v2 protocol - RS485:	**ARCS-W33-A/BT1-7AD/y**
Controlled by OSDP™ v1 & v2 protocol - RS485:	**ARCS-W33-A/BT1-7OS/y**

*Our readers only read the iCLASS™ chip serial number / UID PICO1444-3B. They do not read iCLASS™ cryptographic protection or the HID Global serial number / UID PICO 15693.
**Caution: information about the distance of communication: measured from the center of the antenna, depending on the type of identifier, size of the identifier, operating environment of the reader, temperatures, power supply voltage and reading functions (secure reading).