TOUCHSCREEN / KEYPAD + BIOMETRIC READER

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

Available in standard or keypad versions

11 Awards

BENEFITS

- Customizable multi-function color touchscreen
- Strong multi-factor authentication
- GDPR legislation compliant
- Embedded anti-fraud features
- Interoperable and multi-protocol

Compliant General Data Protection Regulation

OSDP™ Supported by SIA

SSCP® Supported by SPAC

13.56 MHz | BLUETOOTH® | TTL RS485 | EAL5+ | Water resistant EQ IP65

YOUR LOGO

- Display of your logo, images and customized text
- 2 configurable multicolor LEDs

The Architect® Blue biometric reader enhances the security of your access control system and provides strong multi-factor authentication by combining open MIFARE® DESFire® EV2 technologies, a touchscreen / keypad and a fingerprint sensor.

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

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

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.

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!

ADVANCED ANTI-FRAUD FUNCTIONS

- **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.

TOUCH KEYPAD READER

Both a reader and a tactile keypad, it allows user identification by combining the reading of an RFID or virtual card with the input of a personal keypad code.

The same reader can also operate in multiple mode. It authorizes, for example, the reading of cards for personnel and the entry of codes for visitors or temporary workers.

Scramble Pad: protects access against the fraudulent use of identification codes by the random display of the keys.

Mixed display: logo, instructions, personalized messages, images, or keypad are displayed by a simple touch wake-up of the screen.

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

DESIGNED & MADE IN FRANCE

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 Clock&Data (ISO2) or Wiegand output (encrypted communication option - S31) / RS485 output (encrypted option - S33) with SSCP® v1 & v2 secure communication protocols; OSDP™ v1 (plain) and v2 (SCP secure)
Touchscreen	Color touchscreen - 2.8'' - 240 x 320 pixels 12 keys - Standard or random (scramble pad) keypad function / Functions: Card AND Key / Card OR Key Configurable by card (standard or virtual with STid Settings application) or software depending on interface
Decoder compatibility	Compatible with EasySecure interface (encrypted communication)
Reading distances**	Up to 4 cm / 1.57'' with a MIFARE® DESFire® EV2 or Classic 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
Light indicators	2 RGB LEDs - 360 colors ▲ ▲ ▲ Configurable by card (classic or virtual), software or controlled by external command (0V) depending on interface
Audio indicator	Internal buzzer with adjustable intensity Configurable by card (classic or virtual), software or controlled by external command (0V) depending on interface
Relay	Automatic tamper detection management or SSCP® / OSDP™ command according to the interface
Power requirement	Max 370 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
Material	ABS-PC UL-V0 (black)
Dimensions (h x w x d)	166.2 x 80 x 71 mm / 6.53'' x 3.15'' x 2.8'' (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 - 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) and UL
Part numbers	Secure read only - TTL ..... ARCS-R31-F/BT1-xx/1 Secure read only / Secure Plus - TTL ..... ARCS-S31-F/BT1-xx/1 Secure read only - RS485 ..... ARCS-R33-F/BT1-7AB/1 Secure read only / EasySecure interface - RS485 ..... ARCS-R33-F/BT1-7AA/1 Secure read only / Secure Plus - RS485 ..... ARCS-S33-F/BT1-7AB/1 Secure read only / Secure Plus / EasySecure interface - RS485 ..... ARCS-S33-F/BT1-7AA/1 Controlled by SSCP® v1 protocol - RS485 ..... ARCS-W33-F/BT1-7AA/1 Controlled by SSCP® v2 protocol - RS485 ..... ARCS-W33-F/BT1-7AD/1 Controlled by OSDP™ v1 & v2 protocol - RS485 ..... ARCS-W33-F/BT1-7OS/1

DISCOVER THE COMPANION PRODUCTS

13.56 MHz or dual frequency ISO cards & key holders
Bluetooth® & NFC smartphones / smartwatches using STid Mobile ID® application

Privacy filter ANTI-SPY-ARC

SECARD configuration kit and SSCP® v1 & v2 and OSDP™ protocols

Web platform for remote management of your virtual cards

**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.

Headquarters / EMEA
13850 Gréasque, France
Tel.: +33 (0)4 42 12 60 60

PARIS-IDF
92290 Châtenay-Malabry, France
Tel.: +33 (0)1 43 50 11 43

STid UK Ltd.
Gallows Hill, Warwick CV34 6UW, UK
Tel.: +44 (0) 192 621 7884

NORTH AMERICA
Irving, Texas 75063-2670, USA
Tel.: +1 469 524 3442

LATINO AMERICA
San Rafael 06470 CDMX, México
Tel.: +52 (55) 5256 4706

info@stid.com
www.stid-security.com