

# CAPACITIVE KEYPAD + BIOMETRIC READER

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



Available in touchscreen or standard versions



## BENEFITS

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



13.56 MHz



BLUETOOTH®



TTL  
RS485



EAL5+



Water  
resistant  
EQ IP65



YOUR LOGO

- Add your logo
- 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 & EV3 technologies, a capacitive 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 5 identification modes - Prox, long distance or hands-free - to make your access control both secure and instinctive!

## 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.

## VANDAL-PROOF CAPACITIVE KEYPAD

Equipped with a backlit keypad, the reader allows multi-factor identification of users by combining the reading of an RFID or virtual card with the input of a personal keypad code.

Thanks to its different operating modes, the keypad can be used for identification or to activate additional functions (alarm...).

\*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	Secure read only (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)
Decoder compatibility	Compatible with EasySecure interface (encrypted communication)
Keypad	Sensitive / capacitive keypad - 12 backlit keys / Modes: Card AND Key / Card OR Key Configurable by card (classic or virtual with STid Settings application), software or controlled by external command (0V) depending on interface
Reading distances**	Up to 6 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 - Software protection and EAL5+ crypto processor for secure keys storage
Light indicators	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® / OSDP™ command according to the interface
Power requirement	Max 330 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) / ASA-PC-UL-V0 UV (white)
Dimensions (h x w x d)	148.6 x 80 x 71.3 mm / 5.82" x 3.15" x 2.79" (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: case color (l: black - 2 white)	Secure read only - TTL.....ARCS-R31-E/BT1-xx/y Secure read only / Secure Plus - TTL.....ARCS-S31-E/BT1-xx/y Secure read only - RS485.....ARCS-R33-E/BT1-7AB/y Secure read only / EasySecure interface - RS485.....ARCS-R33-E/BT1-7AA/y Secure read only / Secure Plus - RS485.....ARCS-S33-E/BT1-7AB/y Secure read only / Secure Plus / EasySecure interface - RS485.....ARCS-S33-E/BT1-7AA/y  Controlled by SSCP® v1 protocol - RS485.....ARCS-W33-E/BT1-7AA/y Controlled by SSCP® v2 protocol - RS485.....ARCS-W33-E/BT1-7AD/y Controlled by OSDP™ v1 & v2 protocol - RS485.....ARCS-W33-E/BT1-7OS/y

## DISCOVER THE COMPANION PRODUCTS



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



Decorative plate / Spacer /  
Converter cable / Mounting plate...



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



**STid Mobile ID®**  
Online Portal  
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.

Legal: STid, STid Mobile ID®, Architect® and SSCP® are registered trademarks of STid SAS. All trademarks mentioned in this document belong to their respective owners. All rights reserved  
This document is the property of STid. STid reserves the right to make changes to this document and to cease marketing its products and services at any time and without notice. Photos are not contractually binding.

### Headquarters / EMEA

13850 Créasque, 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.

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

### NORTH AMERICA

Irving, Texas 75063-2670, USA  
Tel.: +1 877 894 9135

### LATINO AMERICA

Cuahtémoc, 06600 CDMX, México  
Tel.: +52 (55) 5256 4706

### MIDDLE EAST

Dubai Digital Park, DSO, UAE  
Tel.: +971 521 863 656