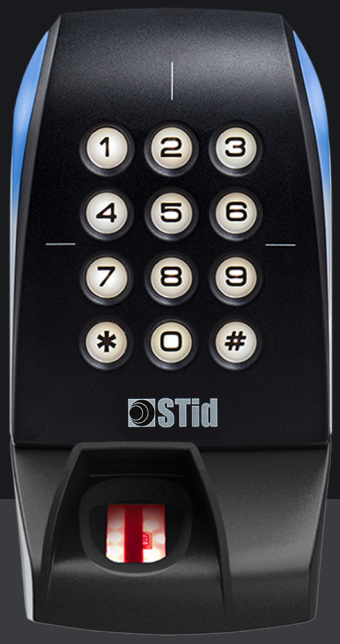
CAPACITIVE KEYPAD + BIOMETRIC READER

MULTI-TECHNOLOGY MIFARE® DESFIRE® EV2 & EV3, NFC SMARTPHONES



Available in touchscreen or standard versions

11 Awards

BENEFITS

- 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

TTL RS485 RS232

Water resistant EQ IP65

YOUR LOGO

- Add your logo
- 2 configurable multicolor LEDs

The Architect® 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* NFC with biometric unlocking or Smartphone only with derogation**

WELCOME TO HIGH SECURITY

The reader uses the latest MIFARE® DESFire® EV2 & EV3 contactless chip technologies with new data security mechanisms:

- **Secure Messaging EV2:** secure transaction method based on AES-128 with protection against interleaving and replay attacks.
- **Proximity Check:** improved protection against relay attacks.

All public encryption algorithms can be used (3DES, AES, RSA, SHA, etc.), which are recommended by official data security agencies (such as the French national agency ANSSI).

VANDAL-PROOF CAPACITIVE KEYPAD

Equipped with a backlit keypad, the reader allows multi-factor identification of users by combining the reading of an RFID 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...).

ADVANCED ANTI-FRAUD FUNCTIONS

The Architect® 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.

*The smartphone can be used as a biometric derogation. No fingerprints are stored in the virtual badge.

DESIGNED & MADE IN FRANCE

WE'VE GOT YOUR BACK

STid

SPECIFICATIONS

Operating frequency / Standards	13.56 MHz: ISO14443 types A & B, ISO18092
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 virtual card)
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
Communication interfaces & protocols	TTL Clock&Data (ISO2) or Wiegand output (encrypted communication option - S31) / RS232 & RS485 outputs (encrypted option - S33) with SSCP® v1 & v2 secure communication protocols; OSDP™ v1 (plain) and v2 (Secure Channel Protocol)
Decoder compatibility	Compatible with EasySecure interface (encrypted communication)
Keypad	Sensitive / capacitive keypad - 12 backlit keys / Modes: Card AND Key / Card OR Key Configuration by card RFID, software or external command (0V) according to the interface
Reading distances**	Up to 6 cm / 3.15'' with a MIFARE® DESFire® EV2 or Classic card
Light indicators	2 RGB LEDs - 360 colors ▲ ▲ ▲ Configuration by card RFID, software or external command (0V) according to the interface
Audio indicator	Internal buzzer Configuration by card RFID, software or external command (0V) according to the interface
Relay	Automatic tamper detection management or SSCP® / OSDP™ command according to the interface
Power requirement	Max 310 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)	148.6 x 80 x 71.3 mm / 5.85'' x 3.14'' 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 ..... ARC-R31-E/PH5-xx/1 Secure read only / Secure Plus - TTL ..... ARC-S31-E/PH5-xx/1 Secure read only - RS485 ..... ARC-R33-E/PH5-7AB/1 Secure read only / EasySecure interface - RS485 ..... ARC-R33-E/PH5-7AA/1 Secure read only / Secure Plus - RS485 ..... ARC-S33-E/PH5-7AB/1 Secure read only / Secure Plus / EasySecure interface - RS485 ..... ARC-S33-E/PH5-7AA/1 Controlled by SSCP® v1 protocol - RS485 ..... ARC-W33-E/PH5-7AA/1 Controlled by SSCP® v2 protocol - RS485 ..... ARC-W33-E/PH5-7AD/1 Controlled by OSDP™ v1 & v2 protocol - RS485 ..... ARC-W33-E/PH5-7OS/1

DISCOVER OUR CREDENTIALS AND OUR ERGONOMIC MANAGEMENT TOOLS

13.56 MHz or dual frequency
ISO cards & key holders

Decorative plate / Spacer /
Converter cables / Mounting plate...

SECARD

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

**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