



DUAL-FREQUENCY KEYPAD READER FOR ACCESS CONTROL



COMPATIBILITY

- ISO14443 types A & B
- MIFARE® credentials
- 125 kHz credentials
- SECard software
- SSCP / OSDP™ protocols



LET YOUR IMAGINATION FLOW

Customizable
of the multicolor LEDs
(RGB, 360 colors)



PRINTING
OF YOUR LOGO
using digital UV
or pad printing



CERTIFICATIONS



OPTIMIZE YOUR TECHNOLOGY MIGRATIONS

STid has designed the Architect® Hybrid 125 kHz + 13.56 MHz vandal proof keypad reader for access control - perfect blend of two identification technologies - to facilitate your migrations to advanced security levels.



MAKE YOUR MIGRATIONS SIMPLE

The Architect® Hybrid keypad reader makes it easy to manage extensions, upgrades and technology migrations. It combines two identification frequencies: 125 kHz (EM, Crosspoint...) and 13.56 MHz (all the MIFARE® chips including DESFire® EV2, NFC, CSN of iCLASS™, CSN of PicoPass®...). If you need to set up a complex multi-site configuration, this reader can be used to read a range of different cards.

MANAGE WITH EASE A MULTI-FACTOR IDENTIFICATION

Both reader and keypad, the device allows a dual-identification by combining card and/or PIN code identifications. Thanks to its various operating modes (card AND key or card OR key), you can use the keypad to identify people or to activate additional functions (activation of the intrusion alarm...).

WELCOME TO HIGH SECURITY

The reader uses the latest MIFARE® DESFire® EV2 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).

CREATE YOUR OWN SCALABLE CONFIGURATION

The Architect® Hybrid can be tailored to your needs, ensuring that all functionalities and security levels can be upgraded across all your readers. The modularity concept allows you to take the 125 kHz module out at the end of your technological migration and / or to implement new functions: touchscreen or biometrics.

STANDING THE TEST OF TIME

Designed to push the boundaries, the Architect® Hybrid keypad reader design has been developed to withstand harsh environments, to operate outside and to offer a high impact resistance (IK08). Thanks to the capacitive technology, the keypad is sealed and protected from the accumulation of dirt. It also prevents the premature mechanical wear of keys, common on conventional keypads available on the market.

SPECIFICATIONS

Operating frequency/Standards	125 kHz 13.56 MHz: ISO14443A types A & B, ISO18092
Chip compatibility	EM42xx / EM4x50 / Wiegand 26, 34, 35 & 37 bits format / Nedap / Crosspoint MIFARE Ultralight® & Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus® & Plus® EV1, MIFARE® DESFire® 256, EV1 & EV2, NFC (HCE), SMART MX, CPS3, PicoPass® (CSN only), iCLASS™ (CSN only)*
Functions	Read only: CSN, private ID (sector/file) or Secure Protocol (Secure Plus) / Secure Read Write
Communication interfaces & protocols	2 variants: - TTL/RS232 protocol: Data Clock (ISO2), Wiegand (ciphered mode Sx1) or RS232 (ciphered mode Sx2) - TTL/RS485 protocol: Data Clock (ISO2), Wiegand (ciphered mode Sx1) or RS485 (ciphered mode Sx3) with secure communication protocols SSCP & SSCP2; OSDP™ V1 (plain communication) & V2 (SCP secure communication) Compatible with EasySecure interface
Keypad	Sensitive / Capacitive keypad - 12 backlit keys - Functions: Card AND Key / Card OR Key Configuration by RFID card, software, external command (0V) or UHF technology according to the interface
Reading distances**	Up to 6 cm / 2.36" with a 125 kHz card / Up to 6 cm / 2.36" with a MIFARE DESFire® EV2 card
Integrated UHF chip	EPC 1 Gen 2 for contactless reader configuration (protocols, LEDs, buzzer...)
Light indicator	RGB LEDs - 360 colors Configuration by RFID card, software, external command (0V) or UHF technology according to the interface
Audio indicator	Internal buzzer Configuration by RFID card, software, external command (0V) or UHF technology according to the interface
Power requirement	190 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)	145.64 x 79.93 x 25.7 mm / 5.71" x 3.11" x 0.98" (general tolerance following ISO NFT 58-000 standard)
Operating temperatures	- 20°C to + 70°C / - 4°F to + 158°F / Humidity: 0 - 95%
Tamper switch	Accelerometer-based tamper detection system with key deletion option (patented)
Protection / Resistance	IP65 Level - Weather-resistant with waterproof electronics (CEI NF EN 61086 homologation) / IK08 reinforced vandal proof structure
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" - External 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, FCC and UL
Part numbers	Secure read only TTL ARC-Rx1-J/BF5-xx/y Secure read only / Secure Plus TTL ARC-Sx1-J/BF5-xx/y Secure read only RS232 ARC-Rx2-J/BF5-5AB/y Secure read only / Secure Plus RS232 ARC-Sx2-J/BF5-5AB/y Secure read only RS485 ARC-Rx3-J/BF5-7AB/y Secure read only Secure Plus RS485 ARC-Sx3-J/BF5-7AB/y Secure read only / EasySecure Interface RS485 ARC-Rx3-J/BF5-7AA/y Secure read only / Secure Plus / EasySecure Interface RS485 ARC-Sx3-J/BF5-7AA/y Secure read write SSCP RS232 ARC-Wx2-J/BF5-5AA/y Secure read write SSCP RS485 ARC-Wx3-J/BF5-7AA/y Secure read write SSCP2 RS485 ARC-Wx3-J/BF5-7AD/y Secure read write OSDP™ RS485 ARC-Wx3-J/BF5-7OS/y

DISCOVER OUR CREDENTIALS



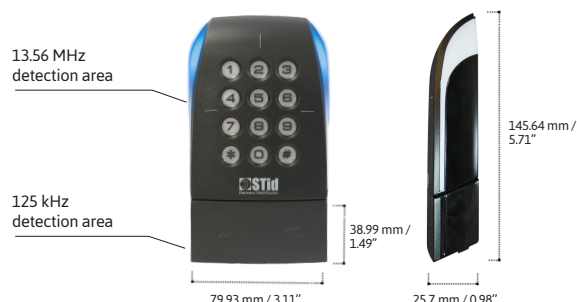
ISO cards
(125 kHz, 13.56 MHz...)



Key holders
(125 kHz, 13.56 MHz...)



SECARD
SECARD configuration kit and
SSCP, SSCP2 & OSDP™ protocols.



*Our readers read only the iCLASS™ UID/Chip Serial Number. They do not read secure HID Global's iCLASS™ cryptographic protections.

**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, power supply voltage and reading functions (secure reading).

Legal statements: STid, STid Mobile ID® and Architect® are trademarks of STid SAS. All other trademarks are property of their respective owners. This document is the exclusive property of STid. STid reserves the right to stop any product or service for any reason and without any liability - Noncontractual photographs.

Headquarters / EMEA

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

PARIS-IDF Office

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

STid UK Ltd. LONDON

Hayes UB11 1FW, UK
Tel.: +44 (0) 192 621 7884

STid UK Ltd.

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

NORTH AMERICA Office

Irving, Texas 75063, USA
Tel.: +1 310 803 2114

LATINO AMERICA Office

Cuahtémoc 06600 CDMX, México
Tel.: +521 (55) 5256 4706

AUSTRALIA / APAC Office

Ultimo, Sydney NSW 2007, Australia
Tel.: +61 (0)2 9274 8853

info@stid.com

www.stid-security.com