



MULTI-TECHNOLOGY KEYPAD READER TO MAKE YOUR MIGRATIONS EASY



COMPATIBILITY



- Bluetooth® & NFC Smartphones
- MIFARE® credentials
- 125 kHz credentials
- SECard software
- SSCP / OSDP™ protocols



LET YOUR IMAGINATION FLOW



CERTIFICATIONS



OPTIMIZE YOUR TECHNOLOGY MIGRATIONS
STid has designed the Architect® Blue Hybrid keypad reader for access control - perfect blend of three identification technologies 125 kHz + 13.56 MHz + Bluetooth® - to facilitate your migrations to advanced security levels.



MAKE YOUR MIGRATIONS SIMPLE

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

INSTINCTIVE ACCESS CONTROL

Your smartphone eliminates the constraints of traditional access control. Choose your favorite identification mode and make your access options both secure and much more instinctive!



Card Mode
Place your smartphone in front of the reader as a standard card.



Slide Mode
Your smartphone turns your hand into a badge you have with you at all times.



Remote Mode
Activate remote control mode to remotely check your access points.



Tap Tap Mode
Tap your smartphone twice in your pocket for close or remote access.



Hands-free Mode
Just walk past the reader! There's nothing else to it!

MANAGE 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.
- Proximity Check: improved protection against relay attacks.

All public encryption algorithms can be used (3DES, AES, RSA, SHA, etc.), recommended.

CREATE YOUR OWN SCALABLE CONFIGURATION

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.

SPECIFICATIONS

Operating frequency/Standards	125 kHz 13.56 MHz: ISO14443A types A & B, ISO18092 Bluetooth®
Chip compatibility	EM42xx / EM4x50 / Format Wiegand 26, 34, 35 and 37 bits / 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)* STid Mobile ID® (virtual card), Orange Pack ID
Functions	Read only: CSN or private ID (sector/file) / Secure Protocol (Secure Plus) / Secure Read Write
Communication interfaces & protocols	TTL protocol Data Clock (ISO2) or Wiegand (ciphered mode Sx1) / 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 card (standard or virtual with STid Settings application), 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 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
Integrated UHF chip	EPC 1 Gen 2 for contactless reader configuration (protocols, LEDs, buzzer...)
Light indicator	RGB LEDs - 360 colors Configuration by card (standard or virtual with STid Settings application), software, external command (0V) or UHF technology according to the interface
Audio indicator	Internal buzzer Configuration by card (standard or virtual with STid Settings application), 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) / Reinforced vandal-proof structure IK08
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, Carlton B120A-UP
Certifications	CE, FCC and UL
Part numbers	Secure read only TTLARCS-Rx1-J/BT2-xx/y Secure read only / Secure Plus TTLARCS-Sx1-J/BT2-xx/y Secure read only RS485ARCS-Rx3-J/BT2-7AB/y Secure read only / Secure Plus RS485ARCS-Sx3-J/BT2-7AB/y Secure read only / EasySecure Interface RS485ARCS-Rx3-J/BT2-7AA/y Secure read only / Secure Plus / EasySecure Interface RS485ARCS-Sx3-J/BT2-7AA/y Secure read write SSCP RS485ARCS-Wx3-J/BT2-7AA/y Secure read write SSCP2 RS485ARCS-Wx3-J/BT2-7AD/y Secure read write OSDP™ RS485ARCS-Wx3-J/BT2-7OS/y

DISCOVER OUR CREDENTIALS



ISO cards & key holders
(125 kHz, 13.56 MHz...)



Bluetooth® & NFC smartphones
using STid Mobile ID® application



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