STid
Electronic Identification

ARCHITECT BLUE

UPGRADABLE HIGH SECURITY READER
SMARTPHONES & RFID CARD

9 Awards

COMPATIBILITY

OSDP™ / SSCP

- Bluetooth® & NFC smartphones
- MIFARE® credentials
- SECard software
- SSCP / OSDP™ protocols

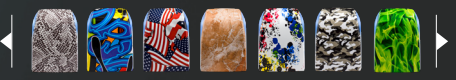
LET YOUR IMAGINATION FLOW

PRINTING OF YOUR LOGO
using digital UV
or pad printing

Customization
of the multicolor LEDs
(RGB, 360 colors)

Casing color

"Skin effect" new customization technology



13.56 MHz | Bluetooth® | Read only | Read / Write | TTL RS485 | EAL5+ | IK10 | Resistant

CERTIFICATIONS

CE FC UL EU c UL us

MOBILE ACCESS READER

Compliant with all access control systems, the Architect® Blue vandal proof reader identifies mobile phones thanks to many Prox or handsfree identification modes. It can work alongside or replace traditional RFID access cards.

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.), and it uses an EAL5+ crypto processor to improve data protection and privacy.

INSTINCTIVE ACCESS CONTROL

Your smartphone becomes your access key by eliminating 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!

CREATE YOUR OWN SCALABLE CONFIGURATION

The Architect® Blue reader 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: keypad or touchscreen.

STANDING THE TEST OF TIME

The Architect® Blue reader design has been developed to withstand harsh environments, to operate outside (IP65 level) and to offer a high vandal proof resistance (IK10 certified).

NXP MIFARE Bluetooth® NFC

www.stid-security.com

SPECIFICATIONS

Operating frequency/Standards	13.56 MHz : ISO14443A types A & B, ISO18092 Bluetooth®
Chip compatibility	MIFARE® Ultralight® & Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus® (S/X) & Plus® EV1, MIFARE® DESFire® 256, EV1 & EV2, CPS3, NFC (HCE), PicoPass® (CSN only), iCLASS™ (CSN only*) STid Mobile ID® (NFC & Bluetooth® 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 S31) / RS485 (ciphered mode S33) with secure communication protocols SSCP & SSCP2 ; OSDP™ V1 (plain communication) & V2 (SCP secure communication) Compatible with EasySecure interface
Reading distances**	Up to 8 cm / 3.15" with a 125 kHz card / Up to 8 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 - EAL5+ secure data storage with certified crypto processor
Integrated UHF chip	EPC 1 Gen 2 for contactless reader configuration (protocols, LEDs, buzzer...)
Light indicator	2 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 with adjustable intensity Configuration by card (standard or virtual with STid Settings application), software, external command (0V) or UHF technology according to the interface
Relay	Automatic tamper direction management or SSCP / OSDP™ command according to the interface
Power requirement	130 mA / 12 VDC typical
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)	106.64 x 80 x 25.70 mm / 4.21" x 3.15" x 1.02" (general tolerance following ISO NFT 58-000 standard)
Operating temperatures	- 30°C to + 70°C / - 22°F to + 158°F / Humidity: 0 - 95%
Tamper switch	Accelerometer-based tamper detection system with key deletion option (patented solution) and/or message to the controller
Protection / Resistance	IP65 Level excluding connector - Weather-resistant with waterproof electronics (CEI NF EN 61086 homologation) Reinforced vandal-proof structure IK10 certified
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, FCC and UL
Part numbers y: case color (1: black - 2: white)	Secure read only - TTL ..... ARCS-R31-A/BT1-xx/y Secure read only / Secure Plus - TTL ..... ARCS-S31-A/BT1-xx/y Secure read only - RS485 ..... ARCS-R33-A/BT1-7AB/y Secure read only EAL5+ / EasySecure Interface - RS485 ..... ARCS-R33-A/BT1-7AA/y Secure read only EAL5+ / Secure Plus - RS485 ..... ARCS-S33-A/BT1-7AB/y Secure read only EAL5+ / Secure Plus / EasySecure Interface - RS485 ..... ARCS-S33-A/BT1-7AA/y Secure read write SSCP - RS485 ..... ARCS-W33-A/BT1-7AA/y Secure read write SSCP2 - RS485 ..... ARCS-W33-A/BT1-7AD/y Secure read write OSDP™ - RS485 ..... ARCS-W33-A/BT1-7OS/y

DISCOVER OUR CREDENTIALS...

13.56 MHz or dual frenquency ISO cards & key holders

Bluetooth® & NFC smartphones using STid Mobile ID® application

...AND OUR ERGONOMIC MANAGEMENT TOOLS

SECard configuration kit and SSCP, SSCP2 & OSDP™ protocols

Web platform for remote management of your virtual badges

*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, temperatures, 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 75063-2670, USA
Tel.: +1 469 524 3442

LATINO AMERICA Office
Cuauhtémoc 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