

IDENTIFICATION EXPERIENCE



Apple Watch Integration

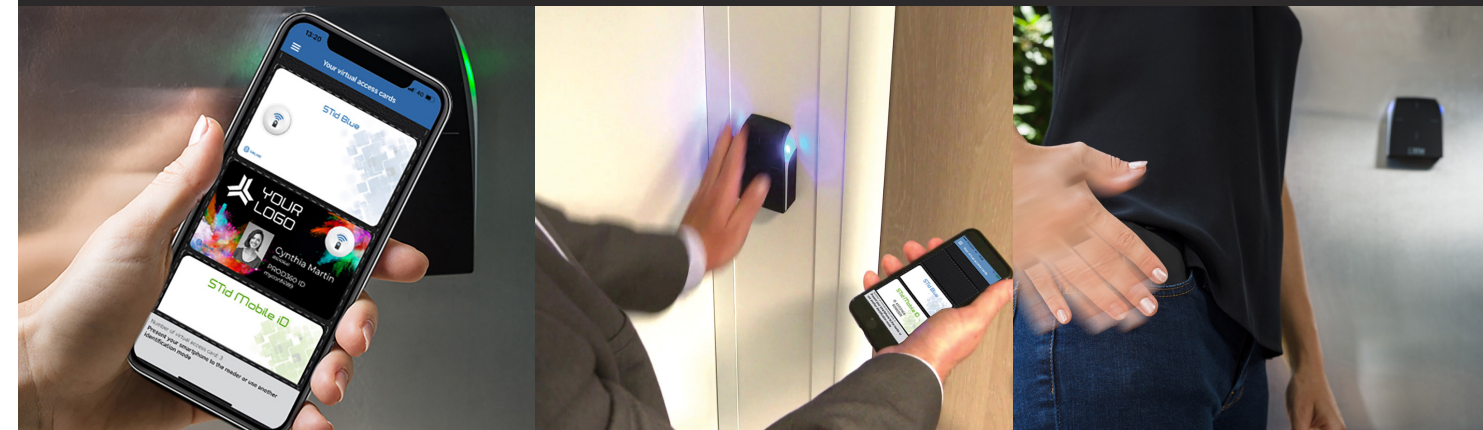
STid Mobile ID® can run on Apple Watch and supports various user interaction modes, bringing an instinctive user experience to iPhone and Apple Watch users.



Your wrist watch transforms into a secure access control card.

6 unique user interaction modes for instinctive contactless identification

Choose your preferred user interaction mode for contactless identification to make your access control more intuitive while keeping it secure.



Badge Mode
Present your smartphone or wearable to the reader like a conventional access card



Slide Mode
Your hand becomes your access card



Tap Tap Mode
Tap tap the smartphone in your pocket to gain access



Remote Mode
Use the "remote button" to conveniently access car parks or other vehicle entrances



Hands-free mode
Simply walk towards the reader without any further action



Voice Command
SIRI voice command on your iPhone (iOS) or Apple Watch

WE'VE GOT YOUR BACK

THE MOBILE & INSTINCTIVE ACCESS CONTROL SOLUTION



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

Cuahtémoc, 06600 CDMX, México
Tel: +52 (55) 19 31 83 36

MIDDLE EAST

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

info@stid.com
www.stid-security.com

Legal Notice: STid, STid Mobile ID® and Architect® are registered trademarks of STid SAS. All trademarks mentioned in this document belong to their respective owners. All rights reserved - This document is the sole property of STid. STid reserves the right, at any time and without notice, to make changes to this document and/or to stop marketing its products and services. The photographs are non-contractual. © STid 2021, all rights reserved / Flyer_STid_Mobile_ID_V6_US

www.stid-security.com

WE'VE GOT YOUR BACK



WHY WOULD YOU HOST ACCESS CARDS ON YOUR SMARTPHONE?



Acceptance of access control

98% of employees consider access control to be obstructive at times. STid Mobile ID® is offering a great user experience, which significantly improves the support of security policies and security systems. The security in private and public organisations benefits from Mobile ID deployments.



In control of your security data

70% of organisations rely on third party infrastructures for their security systems. STid Mobile ID® allows you to be in full control. The platform can run exclusively on your own private network if you prefer.



High security by design

90% of companies believe their data is at risk. STid solutions are secure by design. STid Mobile ID® is based on end-to-end security concepts. Both the storage and communication of data take advantage of modern encryption standards.



Simplified card management

Over 50% of the operational costs of card management are related to printing, customisation and distribution of the cards. STid Mobile ID® significantly reduces these costs by enabling you to create, deliver and revoke virtual cards with just one mouse click.

HIGH SECURITY

Safety via smartphone use

For users, nothing is more convenient than a smartphone to gain access. By default, the smartphone is personal and always at hand whereas traditional physical cards require an additional object to be carried around with the accompanying risk of loss and theft.

Multi-factor authentication

Increase the security level of your installation even further by enforcing that users unlock their smartphone (PIN, biometrics) when accessing the perimeter. In addition it is possible to use Architect Blue readers standard or random keypad module.

Secure data storage

STid Mobile ID® ensures the protection of access data stored in the phone via encryption and authentication methods. STid uses public RGS-compliant algorithms (AES-256 and SHA-2) to encrypt and authenticate data in the application using unique user keys. Security keys are not stored in the application.

ANSSI & FIPS compliant secure exchanges

STid Mobile ID® guarantees data authenticity and data confidentiality at every step of the IT chain: HTTPS - TLS exchanges, mutual authentication for each transaction, uniquely encrypted and signed data exchange...



STid Mobile ID®

COMPATIBLE WITH EXISTING SYSTEMS

EASY TO SET UP

FAST DEPLOYMENT

DESIGNED & MADE IN FRANCE

STid Mobile ID® Portal: 2 secure management methods

Online portal hosted by STid:

- Guaranteed availability of the managed portal 24/7
- CNIL and RGPD certified hosting on servers based in France
- Hosted in certified high-security and monitored datacenters
- No infrastructure costs



Portal hosted within your own infrastructure:

- Possible use of your own data server
- Integration into your IT infrastructure
- Part of your backup and crisis management strategy



Supported by SPAC

The Secure & Smart Communication Protocol (SSCP®) standardizes and secures the communication between physical and logical access control devices.

SPAC® is the European organization, supported by ANSSI, whose mission is to enable the independence and autonomy of organisations in managing their

security by promoting open and sustainable solutions. SPAC® helps promoting the use of the SSCP® protocol throughout Europe to increase international security and safety standards.

The flexible and modular design of Architect® readers supports smooth scenarios for existing access control systems to include STid Mobile ID®.

STid Mobile ID® configuration is fast and does not require on-site software (online portal configuration). No additional programming is required.

Deploy STid Mobile ID® today and start using it without delay. Receive a free virtual access card when you install the STid Mobile ID® application on your smartphone.

WE'VE GOT YOUR BACK

