Secure Identification System

Keep control of your security!

SIS
SECURE IDENTIFICATION SYSTEM

▶ The High Security, by STid!

Access control is all about protecting people, property, valuables and data. The more valuable the items to be protected, the more important it is to have confidence in the system. When choosing a card/reader technology, it is important to state some simple yet fundamental requirements:

- **Not allowing third parties the opportunity to copy or reproduce access badges without supervision.**
- **Not depending on a third party to create your access cards.**
- **Preventing the substitution or emulation of a tag.**

▶ Seamless security

STid has developed the **Secure Identification System** (**SIS**), an easy for implementing a secure information chain to protect your access control application. Security at the heart of the **SIS** is based on the use of private encryption keys. Managing these keys is a **vital issue.**

The **SIS** is used to define, manage and safeguard the encryption keys that protect your data, to ensure:

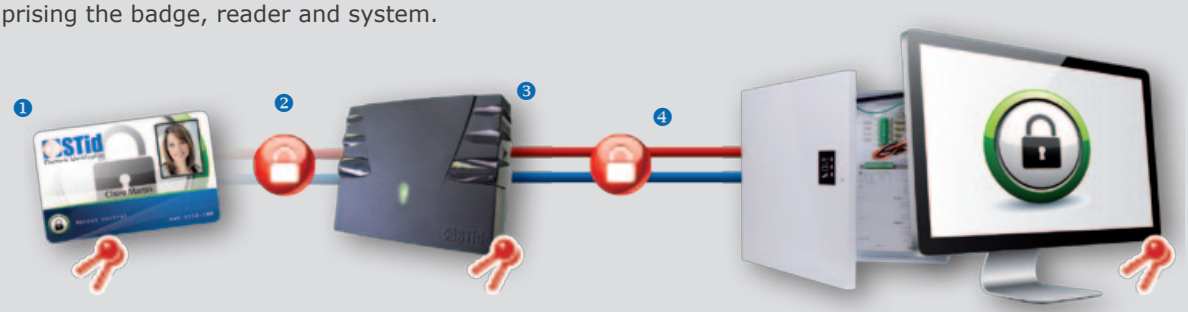
- **Freedom**: define keys and create master badges without needing to use an outside contractor.
- **Confidentiality**: no one needs to know the keys to use or operate them.
- **Independence**: no need to depend on a third party to upgrade the system, card security settings or purchase new cards.

▶ Technological independence

Secure Identification System is open and can be used with all access control systems. It uses tested public security algorithms (TDES, AES, etc.) and interoperable technologies based on international standards (ISO 14443A, ISO 14443-3B, ISO 18092).

▶ High security, a global concept

The ID badge is your key. It's the first link in a security chain, which needs to be consistent and uniform, comprising the badge, reader and system.



1 Data protection of the card
Threat: copy, modification
Countermeasures: secure encoding with public cryptographic algorithms and EAL4+ chips

2 Communication protection between the card and the reader
Threat: interception of data, «replay»
Countermeasures: authentication and encryption

3 Physical and logical protection of the reader
Threat: theft of data
Countermeasures: secure key loading and storage, self-protection

4 Communication protection between the reader and the system
Threat: interception of data, «replay»
Countermeasures: authentication and encryption

Discover our multi-technologies SIS range!

▶ High security reader range

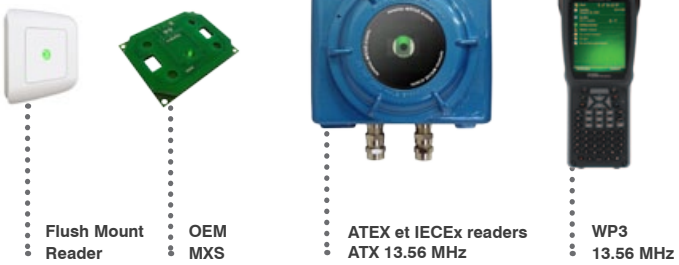
The **SIS** reader range supports many different cards and identification technologies concurrently to help you set up security more easily in your existing systems. It also supports some particular products such as the CPS3 card (IAS protocol), Moneo and NFC transactions.

Readers
LXS / LXE
LXS HYBRID

Keypad readers
LXC

Biometric readers
LDS

Encoders
STR



Flush Mount Reader

OEM
MXS

ATEX et IECEx readers
ATX 13.56 MHz

WP3
13.56 MHz

Smart interfaces
EasySecure
Remote Secure

▶ High security HYBRID reader range

A must-have reader for all technology migration projects!

STid has developed the new **HYBRID** bi-frequency reader range that gives you the best of both worlds for your security applications and migration projects.

All technologies in one reader!

Standard	HYBRID
13.56 MHz	+ 125 kHz
Mifare Ultralight® Mifare Ultralight C® Mifare Classic® Mifare Plus® Mifare DESFire® Mifare DESFire EV1® NFC Famille SMART MX® CPS3 Moneo	EM4102® EM4150® HID® Nedap® Crosspoint / Argina®
	+ 3.25 MHz
	EM4003

As this range of **HYBRID** readers make it possible to simultaneously read the main RFID technologies (125 kHz + 13.56 MHz and 3.25 MHz + 13.56 MHz) it also enables to:

- **Upgrade an existing technology and help it to partially or totally migrate.**
- **Have an optimized management of an inhomogeneous user fleet.**

HID Nedap Argina MIFARE Plus NFC cps3 MIFARE DESFire EV1

Easy, fast and secure implementation!

SECard, the software tool to keep control of your security

The key element of your security consists in integrally and independently managing the parameters related to your system. We thus help you master your security by providing you with everything you need in terms of contactless identification applications (key choice, data protection parameters, etc.).

The SECard software can be used installation and integration contractor and other users to easily:

- **Create master cards for programming readers,**
- **Securely program user cards,**
- **Manage security configurations.**

Easy implementation

1. Create the configuration card and define the encryption keys.
2. Program the user cards with the specified encryption keys.
3. Program the readers with my configuration card - they will now only read my cards.

SSCP Secure Communication Protocol

The open protocol **SSCP** (STid Secure Common Protocol) uses data encryption (AES) and two-way "reader-controller" authentication to ensure security before any communication is allowed between the reader and management system.

- **Open, non-secret protocol**
- **Cryptography using public algorithms** (AES, HMAC, etc.)
- **Reader authentication** (session key)
- **Signature, encryption**
- **User key management**
- **Selectable communication modes and security**
- (plain, signed, encrypted, signed and encrypted)

Memo

Benefits: Full control over security

- Protection and confidentiality: user badges and master badge protected, Security keys remain confidential.
- Standalone management: autonomous programming of user badges, configure and reconfigure readers as you wish.

Modular and scalable architectures for an easy integration!

The **SIS** range offers various options for connecting your systems. In many cases, you can simply “Plug & Play”, meaning major technological upgrades can be implemented in terms of badges and identification, without jeopardising the system.

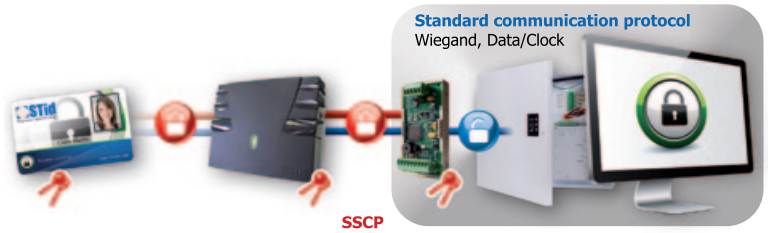
1 Secure read only

Secure communication
Crypto 1, 3DES, AES...

Standard communication protocol
TTL (Wiegand, Data/Clock), RS232, RS485
Secure communication option (S31, S32, S33)

The reader is autonomous to communicate with the card. Architecture compatible with all access control systems in the market, without any development.

2 Secure read only and secure communication with EasySecure decoder



Standard communication protocol
Wiegand, Data/Clock

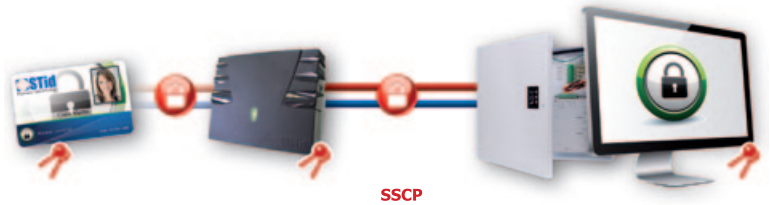
Secure communication
Crypto 1, 3DES, AES...

SSCP
Secure protocol
RS485

Safe area

Decoder / Converter installed in a safe area (access control panel) and supporting the SSCP protocol. Architecture compatible - Plug & Play - with all access control systems in the market, without any development.

3 Secure read/write



Secure communication
Crypto 1, 3DES, AES...

SSCP
Secure protocol
RS232, RS485, USB

Fully secure access control system. The reader is fully managed by the system.

4 Transparent reader with RemoteSecure interface

SSCP Secure protocol
RS232, RS485

Secure communication
DES, 3DES, AES / CMAC-AES

Safe area

Security mechanisms are located in the RemoteSecure interface. The reader is “transparent” and does not contain any keys.

Flyer_SIS_v1.00_US

Approved STid reseller

Headquarters
20 Parc d’activités des Pradeaux
13850 Gréasque, FRANCE
+33 (0)4 42 12 60 60
+33 (0)4 42 12 60 61
info@stid.com

Paris - IDF Agency
Immeuble Le Fahrenheit
28, rue de la Redoute
92260 Fontenay-aux-Roses, FRANCE
+33 (0)1 43 50 11 43
+33 (0)1 43 50 27 37
info@stid.com

STid America
Puebla #398, Interior
302 Piso 3 - Col.Roma
C.P.06700 México D.F.
+52 (55) 52 56 47 06
+52 (55) 52 56 47 07
info@stid-america.com