

LECTEUR DE BADGES RFID + BIOMÉTRIE

MULTI-TECHNOLOGIE MIFARE® DESFIRE® EV2 & EV3 ET SMARTPHONES NFC



Disponible en version écran tactile ou clavier



BÉNÉFICES

- Authentification forte multi-facteur
- Conforme à la législation européenne RGPD & française CNIL
- Fonctions anti-fraudes avancées
- Interopérable et multi-protocole

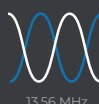
Conforme



Supporté par SIA



Supporté par SPAC



13,56 MHz



Résistant à l'eau IP65



- Impression de votre logo
- 2 LEDs multicolores paramétrables

En associant les dernières technologies MIFARE® DESFire® EV2 à un capteur d'empreintes digitales, le lecteur biométrique Architect® assure une authentification forte de l'utilisateur et renforce la sécurité de votre système de contrôle d'accès.

GESTION SÉCURISÉE & SIMPLIFIÉE DES EMPREINTES BIOMÉTRIQUES

Différentes possibilités de gestion des empreintes digitales en fonction de vos besoins :

- **Stockage des données biométriques dans le badge RFID** (conformité avec la législation française CNIL & européenne RGPD)
- **Stockage des données dans le système de contrôle d'accès**
- **Mode badge seul avec dérogation au niveau du badge d'accès** (gestion des visiteurs ponctuels, doigts difficiles, etc.)
- **Smartphone* NFC avec déverrouillage biométrique obligatoire ou mode smartphone seul avec dérogation**

BIENVENUE DANS LA HAUTE SÉCURITÉ

Le lecteur supporte les dernières technologies de puces sans contact MIFARE® DESFire® EV2 & EV3 avec leurs nouveaux dispositifs de sécurisation des données :

- **Secure Messaging EV2** : méthode de sécurisation des transactions qui protège contre les attaques par entrelacement et par rejeu.
- **Proximity Check** : protection contre les attaques relais.

Il permet d'utiliser des algorithmes de sécurité publics (3DES, AES, RSA, SHA...) reconnus par les organismes spécialisés et indépendants dans la sécurité de l'information (ANSSI).

MEILLEURE AUTOPROTECTION DU MARCHÉ

Le système breveté de détection d'arrachement par capteur de mouvement protège les données sensibles en permettant d'effacer les clés d'authentification.

Contrairement aux solutions existantes du marché, la fiabilité de l'accéléromètre évite tout contournement du système.





FONCTIONS ANTI-FRAUDES AVANCÉES

Le lecteur biométrique Architect® est conçu pour résister aux tentatives de fraudes :

- **Détection de faux doigts** : le lecteur détecte un large panel d'empreintes digitales contrefaites en latex, Kapton, film transparent, caoutchouc, graphite, etc.
- **Détection de doigts morts**
- **Doigt sous contrainte** : l'administrateur peut attribuer un numéro de doigt dédié à l'authentification et envoyer une alerte au système face à une menace.

*Le smartphone peut être utilisé comme une dérogation biométrique. Aucune empreinte digitale n'est stockée dans le badge virtuel.

CARACTÉRISTIQUES

Fréquences porteuses / Normes	13,56 MHz : ISO14443 types A & B, ISO18092
Compatibilités puces	MIFARE® Classic & Classic EV1 (4 ko), MIFARE® Plus® (S/X) & Plus® EV1, MIFARE® DESFire® 256 (1 empreinte), EV1, EV2 & EV3 STid Mobile ID® (badge virtuel NFC)
Modes	Lecture seule CSN et sécurisée (fichier, secteur) / Piloté par protocole (lecture écriture)
Capteur d'empreintes digitales	Optique (SAFRAN MorphoSmart™ CBM E3) - ≤ 1 seconde pour une authentification 1:1 Empreinte digitale stockée dans le badge RFID ou dans le système
Interfaces & protocoles de communication	Sortie TTL Data/Clock (ISO2) ou Wiegand (option communication chiffrée - S31) / Sorties RS232 & RS485 (option chiffrée - S33) avec protocoles de communication sécurisés SSCP® v1 & v2 ; OSDPTM v1 (en clair) et v2 (Secure Channel Protocol)
Compatibilité décodeurs	Compatible avec l'interface EasySecure (communication chiffrée)
Distances de lecture**	Jusqu'à 8 cm avec un badge MIFARE® DESFire® EV2 ou Classic
Indicateurs lumineux	2 LEDs RVB - 360 couleurs ▲ ▲ ▲ Configurable par badge RFID, logiciel ou piloté par commande externe (0V) selon interface
Indicateur sonore	Buzzer intégré Configurable par badge RFID, logiciel ou piloté par commande externe (0V) selon interface
Relais	Gestion anti-arrachement automatique ou piloté par commande OSDPTM ou SSCP® selon interface
Consommation	280 mA / 12 VDC max
Alimentation	7 VDC à 28 VDC
Connectique	Bornier débrochable 10 points (5 mm) - Bornier débrochable 2 points (5 mm) ; contact O/F - Indicateur d'état d'arrachement
Matériaux	ABS-PC UL-V0 (noir)
Dimensions (h x l x p)	148,6 x 80 x 71,3 mm (tolérance générale suivant standard ISO NFT 58-000)
Températures de fonctionnement	- 10°C à + 50°C
Fonction anti-arrachement	Détection arrachement par accéléromètre avec possibilité d'effacement des clés (breveté) et/ou message au contrôleur
Protection / Résistance	IP65 - Résistant aux intempéries, à l'eau et aux poussières (certification CEI NF EN 61086) Humidité : 0 - 95%
Fixation	Montage sur tout type de support y compris sur métal sans spacer - Murale en applique / sur pots électriques : - Européen 60 & 62 mm - Américain (métallique/plastique) - 83,3 mm - Dimensions : 101,6 x 53,8 x 57,15 mm - Exemples : Hubbel-Raco 674, Carlon B120A-UP
Certifications    	CE (Europe), FCC (USA), IC (Canada) et UL
Codes Articles	Lecture seule sécurisée - TTL.....ARC-R31-D/PH5-xx/1 Lecture seule sécurisée / Secure Plus - TTL.....ARC-S31-D/PH5-xx/1 Lecture seule sécurisée - RS485.....ARC-R33-D/PH5-7AB/1 Lecture seule sécurisée / Décodeur EasySecure - RS485.....ARC-R33-D/PH5-7AA/1 Lecture seule sécurisée / Secure Plus - RS485.....ARC-S33-D/PH5-7AB/1 Lecture seule sécurisée / Secure Plus / Décodeur EasySecure - RS485.....ARC-S33-D/PH5-7AA/1 Piloté par protocole SSCP® v1 - RS485.....ARC-W33-D/PH5-7AA/1 Piloté par protocole SSCP® v2 - RS485.....ARC-W33-D/PH5-7AD/1 Piloté par protocole OSDPTM v1 & v2 - RS485.....ARC-W33-D/PH5-7OS/1

DÉCOUVREZ NOS IDENTIFIANTS ET NOS OUTILS ERGONOMIQUES DE GESTION



Badges ISO & porte-clés
13,56 MHz ou bi-fréquences



Plaque d'embellissement / Spacer /
Câbles convertisseurs / Plaque de renfort...



SECARD
Kit de programmation SECARD et
les protocoles SSCP® v1 & v2 et OSDPTM

**Attention : informations sur les distances de communication : mesurées au centre de l'antenne, dépendant de la configuration de l'antenne, de l'environnement d'installation du lecteur, de la température, de la tension d'alimentation et du mode de lecture (sécurisé ou non). Des perturbations externes peuvent provoquer la diminution des distances de lecture.
Mentions légales : STid, Architect® et SSCP® sont des marques déposées de STid SAS. Toutes les marques citées dans le présent document appartiennent à leurs propriétaires respectifs. Tous droits réservés - Ce document est l'entière propriété de STid. STid se réserve le droit, à tout moment et ce sans préavis, d'apporter des modifications sur le présent document et/ou d'arrêter la commercialisation de ses produits et services. Photographies non contractuelles

Siège Social / EMEA

13850 Créasque, France
Tél. : +33 (0)4 42 12 60 60

PARIS-IDF

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

STid UK Ltd.

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

AMÉRIQUE DU NORD

Irving, Texas 75063-2670, USA
Tél. : +1 469 524 3442

AMÉRIQUE LATINE

San Rafael 06470 CDMX, México
Tél. : +52 (55) 5256 4706

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