MorphoAccess® VP Series

Guide Utilisateur

Osny, France

Avertissement

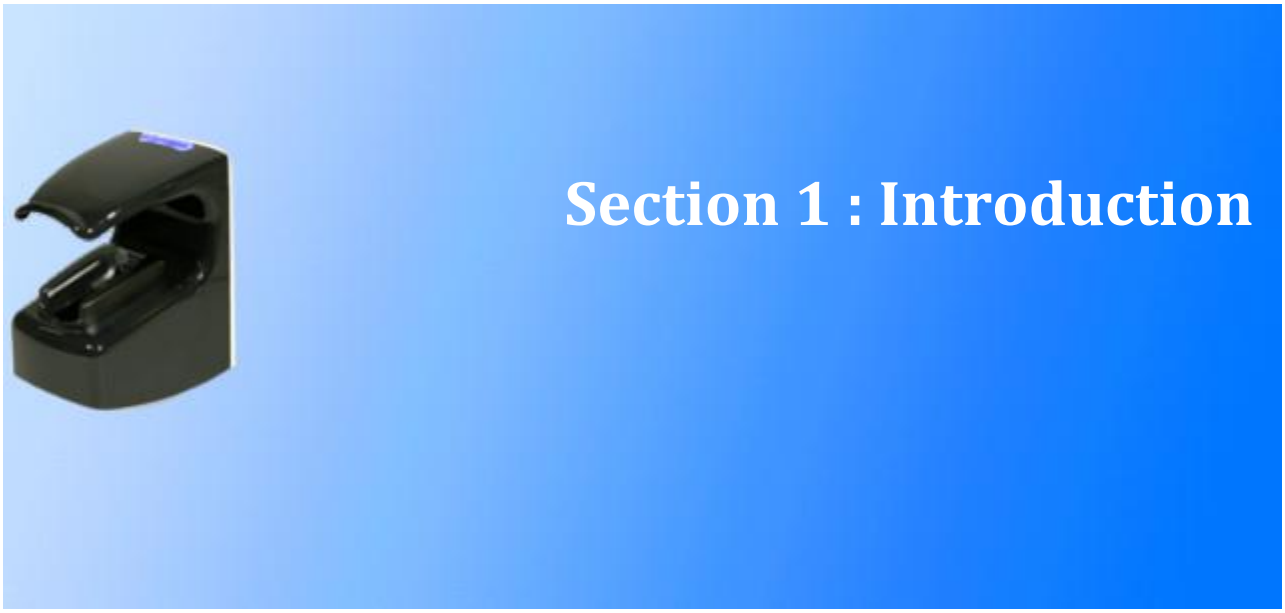
Historique de révision

Le tableau ci-dessous contient l'historique des modifications apportées au présent document.

Version	Date	Description
01	Mai 2011	Création du document
02	Février 2012	Support des cartes DESFire® EV1 AES Gestion de 65000 transactions

Sommaire

Liste des illustrations



Section 1 : Introduction

Terminal MorphoAccess® VP Series

Nous vous remercions d'avoir choisi un terminal de la Série MorphoAccess® VP, première gamme de terminaux de contrôle d'accès physique à intégrer la technologie de reconnaissance multimodale combinant la biométrie du réseau veineux du doigt et celle de l'empreinte digitale.

Ces terminaux apportent au contrôle d'accès physique les atouts de la multimodalité veine/empreinte :

- l'ouverture du contrôle biométrique aux personnes qui rencontraient jusqu'alors des difficultés à utiliser les dispositifs biométriques exploitant une seule modalité
- un excellent ratio entre taux de faux rejets (FRR) et taux de fausses acceptations (FAR), ce permet de garantir un niveau de sécurité très élevé sans pour autant affecter le confort d'utilisation / le taux de service du terminal
- une résistance accrue à la fraude (en combinant les mécanismes de protection propres à chaque technologie et en mettant à profit de nouvelles caractéristiques issues de la fusion des deux biométries)
- tout en offrant la même ergonomie d'utilisation que celle qui a fait que les systèmes basés sur l'empreinte digitale ont été rapidement adoptés par les utilisateurs.

De plus, les terminaux de la Série MorphoAccess® VP ont été conçus en ayant à l'esprit deux concepts majeurs :

- attractivité du design (choix des textures, qualité des finitions…),
- et aspect pratique, tant au montage qu'à la connexion.

Pour toutes ces raisons, nous sommes convaincus que les terminaux de la Série MorphoAccess® VP répondront aux attentes de nos partenaires les plus exigeants, en tant que solution ultime pour la précision, la performance et la sécurité de leurs équipements !

Afin de garantir l'utilisation la plus efficace de votre terminal MorphoAccess® VP, nous vous recommandons de lire entièrement et attentivement ce Guide d'Utilisation.

Champ d'application du document

Ce guide porte sur l'utilisation des terminaux de la Série MorphoAccess® VP, qui est composé des produits suivants :

Terminaux		Biométrie multimodale veine/empreinte	Lecteur de cartes à puce sans contact	
			MIFARE®	DESFire®
Série MorphoAccess® VP	MorphoAccess® VP-Bio	x		
	MorphoAccess® VP-Dual	x	x	x

Consignes de sécurité

L'installation de ce produit doit être réalisée par un technicien qualifié et être conforme à toutes les réglementations locales.

Il est fortement recommandé d'utiliser une alimentation électrique de classe II de 12 V [9V-16V] et 1 A minimum conformément aux règles du type très basse tension de sécurité (TBTS). Le câble d'alimentation électrique 12 V n'excédera pas 10 mètres.

Ce produit est destiné à être installé sur une alimentation électrique conforme à la norme EN60950, conformément aux exigences NEC Classe 2 ; ou alimenté par un bloc d'alimentation externe listé EN60950 et marqué Classe 2, Limited Power source, ou LPS (source de puissance limitée) et de charge nominale 12 VCC, 1 A minimum.

En cas de raccordement de bâtiment à bâtiment, il est recommandé de raccorder le 0 V à la terre. Le câble de terre doit être raccordé à la borne 0 V GND.

Veuillez noter que tous les branchements du terminal MorphoAccess® VP décrits ci-après sont de type TBTS (très basse tension de sécurité).

Informations pour l'Europe

Morpho déclare par la présente que le terminal MorphoAccess® VP a été testé et jugé conforme aux normes citées ci-après : EN302 291-2 V.1.1.1 (07-2005), la recommandation 1999/519/CE avec les normes EN 50364 ; EN 301 489-3 V.1.4.1 (02) et la Directive sur les basses tensions 2006/ 95/CE : CEI60950-1:2005 2ème édition.

Informations pour les États-Unis

Ce dispositif est conforme à la partie 15 des Règles FCC. Le fonctionnement est soumis aux deux conditions suivantes : (1) ce dispositif ne peut pas provoquer d'interférences nuisibles et (2) ce dispositif doit accepter toutes les interférences reçues, y compris les interférences provoquant un fonctionnement involontaire.

Les changements ou les modifications qui n'ont pas été formellement approuvés par la partie responsable de la conformité pourraient annuler l'autorité de l'utilisateur quant au fonctionnement de l'équipement.

Partie responsable :

Morpho

Le Ponant de Paris, 27, rue Leblanc

F 75512 PARIS CEDEX 15

FRANCE.

NOTE

Cet équipement a été testé et jugé conforme aux limites pour un dispositif numérique de Classe B, conformément à la partie 15 des Règles FCC. Ces limites sont conçues pour fournir une protection appropriée contre les interférences nuisibles au sein d'une installation résidentielle. Cet équipement génère, utilise et peut émettre une puissance de fréquence radio et, s'il n'est pas installé et utilisé conformément aux instructions, il peut provoquer des interférences nuisibles aux communications radio. Cependant, il n'y a aucune garantie qu'aucune interférence ne se produira dans une installation particulière. Si cet équipement provoque des interférences nuisibles lors de la réception de la télévision ou de la radio, ce que l'on peut déterminer en mettant l'équipement hors tension ou sous tension, l'utilisateur est encouragé à essayer de corriger l'interférence en suivant une ou plusieurs des mesures suivantes :

- réorienter ou déplacer l'antenne de réception,
- augmenter la distance entre l'équipement et le récepteur,
- brancher l'équipement à l'intérieur d'une sortie sur un circuit différent de celui sur lequel le récepteur est branché,
- consulter le fournisseur ou un technicien radio / télévision expérimenté pour toute aide.

Des câbles blindés doivent être utilisés avec cette unité afin d'assurer la conformité aux limites de la classe B FCC.

Préambule

Quelques notions sur la biométrie empreinte digitale

Les empreintes digitales sont permanentes et uniques. Elles se forment avant la naissance et perdurent pendant toute la vie d'un individu. La classification et la comparaison d'empreintes digitales, à des fins diverses, sont pratiquées depuis la fin du 19ème siècle.

La peau du dessous des doigts diffère des autres zones du corps. Cette peau présente des lignes en relief qui sont appelées crêtes (Ridges).

Une crête ne va pas d'un côté à l'autre de manière continue, en fait une crête peut s'incurver, se terminer (fin), ou se séparer en deux ou plus nouvelles crêtes (bifurcations). La disposition des crêtes est permanente, ignorant mutilations accidentelles ou intentionnelles.

Les empreintes digitales peuvent être classées suivant les principales formes que peut prendre une crête, comme une spire (Whorl), une boucle (Loop), des arches, etc. Des caractéristiques uniques, appelées **Minuties**, identifient ces points d'une empreinte digitale, là où les crêtes bifurquent ou se terminent, comme illustré dans la **Figure 1**. Ces minuties sont les caractéristiques uniques qui forment la base de tout système utilisant des techniques de comparaison d'empreinte digitale à des fins de vérification et l'identification.

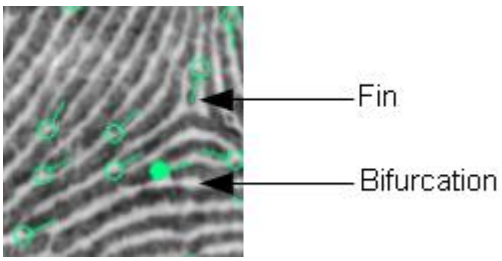


Figure 1: Les minuties sont classées en deux catégories : fin de crête et bifurcation

La biométrie basée sur l'empreinte digitale est une technologie mature, utilisée pour de nombreuses applications, car elle offre un excellent compromis entre nombre de critères comme l'acceptation par les utilisateurs, la facilité d'utilisation, la performance, la stabilité, le coût et l'interopérabilité.

Depuis le début des années quatre-vingt, Morpho étudie les caractéristiques des empreintes digitales et améliore constamment son expertise de la technologie d'identification à base d'empreintes digitales. Morpho a d'abord développé des systèmes automatiques d'identification d'empreintes digitales (AFIS), puis appliqué ensuite ce savoir-faire unique et sa position de leader mondial à de nombreux marchés comme celui du contrôle d'accès physique (accès aux locaux), du contrôle d'accès logique (accès aux ordinateurs et aux réseaux), du paiement sécurisé ou des applications OEM.

Quelques notions sur la biométrie du réseau veineux du doigt

La reconnaissance du motif vasculaire est une activité relativement récente dans le domaine de la biométrie. Cela tient au fait que ce n'est que récemment que l'on a été en mesure d'observer d'une façon pratique et non-intrusive le réseau vasculaire d'un être humain vivant. Le premier article ouvrant la voie à ce type d'observation a été publié au début des années quatre-vingt-dix.

A l'instar des empreintes digitales, la formation du réseau vasculaire est régie par de nombreux phénomènes, qui concourent à donner au réseau sa forme « finale ». Par conséquent, la communauté médicale dans son ensemble considère que le réseau vasculaire est unique pour chaque individu. La recherche suggère que le réseau vasculaire peut varier au cours de la vie d'un individu, mais que ce processus est extrêmement lent et que tout changement significatif de ce réseau a des conséquences dramatiques sur les fonctions vitales de l'organisme.

Les caractéristiques spécifiques du réseau vasculaire, alliées aux récents progrès en matière de techniques d'acquisition, en font un excellent candidat pour l'authentification et l'identification biométriques.

Le principe de base de l'acquisition du réseau vasculaire consiste à sélectionner une longueur d'onde d'illumination pour laquelle l'absorption d'hémoglobine désoxygénée (qui circule librement dans le système sanguin) sera maximale et l'absorption de « fond » (tous les autres tissus cellulaires) sera minimale. De cette façon, le réseau vasculaire apparaît de manière très contrastée « à travers » les différentes couches de peau du doigt.

L'image acquise est alors traitée au moyen de techniques de traitement d'image classiques pour améliorer le signal utile et diminuer le bruit, jusqu'à obtenir un nombre réduit de niveaux gris adapté à des comparaisons performantes (**Figure 2**).

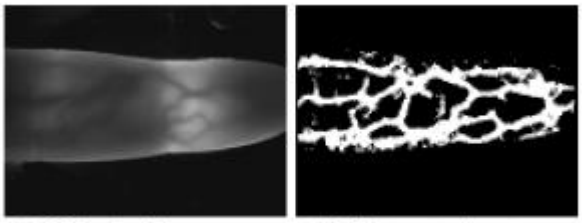


Figure 2: Traitement de l'image d'un réseau veineux
Source: "Finger Vein Authentication technology and financial applications" par M. Himaga et K. Kou

De nos jours, la technologie de reconnaissance de veine est l'une des technologies biométriques disponibles les plus fiables et les plus faciles à mettre en œuvre. Un de ses atouts majeurs est sa résistance à la contrefaçon. Frauder la reconnaissance du réseau veineux est très difficile, ceci pour deux raisons : 1/ l'information utile est située sous la peau, donc impossible à acquérir à l'insu de son propriétaire, et 2/ les techniques d'éclairage et d'imagerie nécessitent des caractéristiques spécifiques de vaisseaux sanguins pour former une image utilisable d'un point de vue biométrique.

La technologie mise en œuvre dans les terminaux MorphoAccess® VP est basée sur une technologie brevetée par Hitachi.

La Multimodalité et ses avantages

Les performances en termes de précision (caractérisée par les rapports FRR et FAR) demeurent l'un des principaux challenges de l'industrie biométrique.

Mais à partir du moment où une technologie biométrique a atteint la maturité, le temps et les efforts nécessaires pour l'améliorer (par exemple en affinant les algorithmes) sont de plus en plus importants. A titre d'exemple, les évaluations du NIST (National Institute of Standards and Technology) relatives à la technologie de reconnaissance d'empreintes digitales montrent que gagner un point en termes de précision prend des années aux meilleurs algorithmes.

Aussi a-t'on recherché différentes approches alternatives à l'amélioration d'une seule technologie.

La première consiste à utiliser plusieurs échantillons de même nature biométrique (par exemple les 10 doigts d'un individu, comme dans les systèmes AFIS). Cette technique est connue sous le nom de « multi-biométrie », ou « multi-instances ». Cette méthode produit des améliorations significatives, mais la phase d'acquisition et le temps de traitement sont considérablement allongés, impactant considérablement le coût (sans oublier le fait que l'universalité n'est pas garantie : par exemple, tous les individus ne présentent pas 10 doigts utilisables).

Une autre voie est d'utiliser plusieurs algorithmes pour traiter le même jeu de données biométriques (approche dite « multi-algorithmes »). Cette méthode n'est efficace que lorsqu'elle est appliquée à des algorithmes qui ne se montrent pas assez performants par eux-mêmes, et elle est également gourmande en temps de traitement.

C'est pourquoi ces dernières années, l'industrie biométrique s'est tournée vers une approche innovante - la **Multimodalité** - qui consiste à combiner deux biométries complémentaires. Les études préliminaires menées sur le sujet ont en effet montré que ce concept pourrait améliorer les performances dans une mesure bien plus grande que n'importe laquelle des autres approches considérées jusqu'ici. Cet objectif est atteint plus particulièrement lorsque l'on capture puis traite les deux jeux de données biométriques en même temps, avec un terminal unique.

Morpho a été un pionnier dans ce domaine, pariant très tôt sur la combinaison entre les technologies de reconnaissance de l'empreinte digitale et du réseau veineux du doigt. En effet, Morpho a compris que ces deux biométries étaient particulièrement adaptées à une fusion efficace :

- Elles sont matures, stables et surtout indépendantes l'une de l'autre.
- Les deux jeux de données biométriques peuvent être capturés ensemble par un seul et même terminal, sans nécessiter d'évolution technique radicale, préservant ainsi le coût de la solution.

- L'acquisition peut se faire avec la même ergonomie que pour l'empreinte digitale, qui est plébiscitée pour sa facilité d'utilisation et largement déployée dans le monde pour cette raison.

Après avoir établi un partenariat avec Hitachi - pour sa parfaite connaissance de la technologie d'imagerie de la veine du doigt - Morpho a développé le premier terminal multimodal (veine + empreinte) du marché : le MorphoSmart™ FINGER VP, qui existe en version OEM et en version DESKTOP.

La technologie multimodale veine/empreinte développée par Morpho présente de nombreux atouts:

- Elle permet d'adresser les personnes qui ont habituellement des difficultés à s'enrôler avec un terminal monomodal. Le taux de FTE (Failure to Enroll) obtenu est proche du produit des taux de FTE de chaque mode (FTEmode1 x FTEmode2).
- La précision est considérablement améliorée, réduisant la probabilité de rejeter des individus par erreur et d'accepter des imposteurs. Grâce à un Taux de Faux Rejet très bas (FRR) même pour des Taux de Fausse Acceptation (FAR) très exigeants (pour un FAR=10^{-4}, le FRR multimodal est dix fois plus bas que celui de la meilleure modalité), cette technologie apporte une parfaite réponse aux exigences de confort d'utilisation et de sécurité demandées par toute application biométrique.
- La résistance à la fraude est améliorée en conjuguant les mécanismes de protection inhérents à chaque biométrie mais aussi en exploitant de nouvelles caractéristiques issues de la fusion.

La gamme de produits biométriques multimodaux de Morpho s'étend maintenant aux terminaux de Contrôle d'Accès Physique, avec la Série MorphoAccess® VP, qui bénéficie de toutes ces avancées.

Principes d'acquisition

Zones utiles

Le terminal est conçu pour capturer la zone la plus riche en données biométriques utiles :

- pour l'empreinte digitale, elle se situe habituellement au centre de la première phalange.
- pour le réseau veineux, elle se situe habituellement entre la première et la troisième phalange.

Ceci est résumé dans la figure ci-dessous.

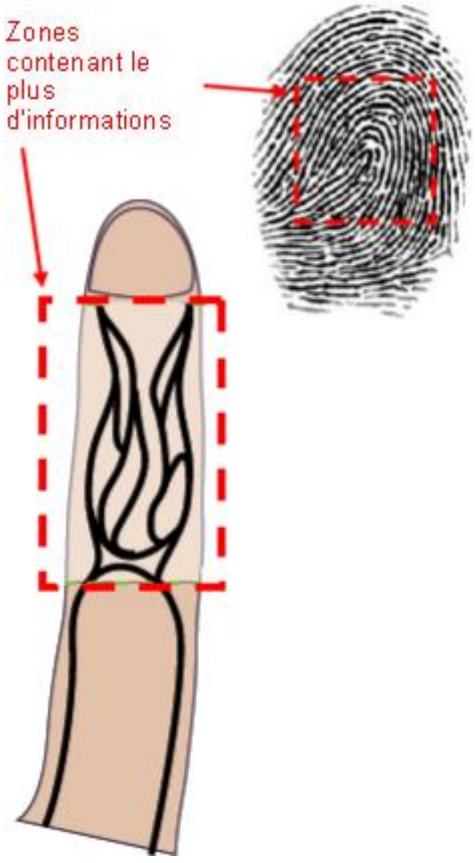


Figure 3: Zones utiles

Ergonomie d'acquisition

La capture d'image est effectuée avec une caméra CMOS. La méthode d'acquisition d'images dépend de la nature des données biométriques à acquérir.

L'acquisition de l'image de l'empreinte digitale nécessite que la première phalange du doigt (zone ou se trouve l'empreinte digitale, voir **Figure 3**) soit en contact avec la zone dédiée du capteur (zone carrée en haut de la surface transparente).

Le guide de bout de doigt **(1)** a été spécialement conçu pour aider l'utilisateur à placer le centre de l'empreinte digitale dans la zone de capture de l'empreinte **(2)**.

Par contre, l'acquisition de l'image du réseau veineux nécessite que la deuxième phalange du doigt ne pas soit en contact avec la zone dédiée du capteur. Le deuxième guide-doigt **(3)** a été spécialement conçu pour tenir le doigt dans une position droite pour éviter tout contact avec la surface de capture de l'image du réseau veineux.

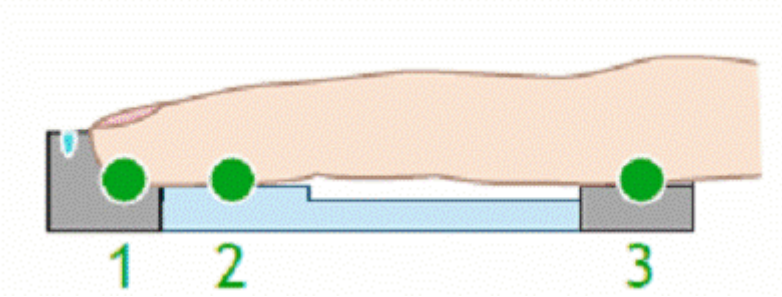


Figure 4: Vue en coupe de la zone d'acquisition

Pour obtenir la meilleure qualité d'image possible, il est fortement recommandé d'essuyer la surface transparente du capteur avec un tissu sec, lorsque celle-ci est humide.

Doigts recommandés

Nos terminaux ont été conçus spécifiquement pour l'utilisation de trois doigts : le majeur, l'index, et l'annulaire. Ce sont donc ces 3 doigts qui sont recommandés pour obtenir les meilleurs résultats pendant l'acquisition (voir Figure 5).

Figure 5: Doigts recommandés pour la capture

Processus d'Enrôlement

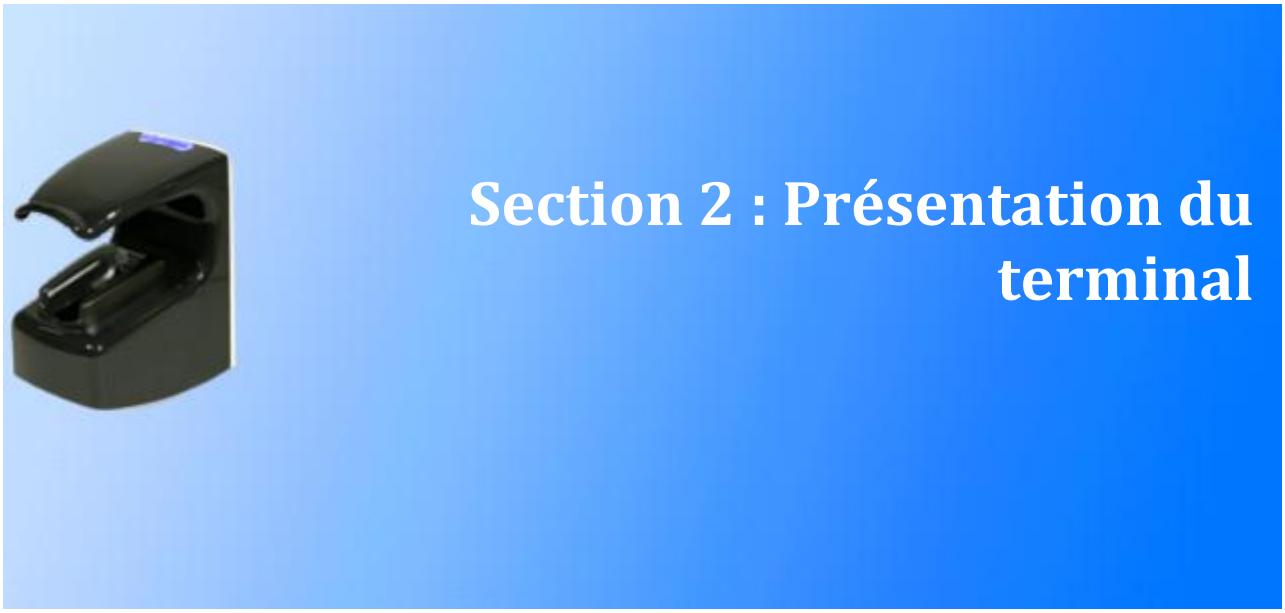
Les précautions prisent pendant la phase d'enrôlement influent directement sur toutes les étapes suivantes de la chaîne de reconnaissance biométrique.

Aussi est-il fortement recommandé d'expliquer aux utilisateurs lors de la phase d'enrôlement comment poser le doigt sur le terminal de façon adéquate, afin d'acquérir la meilleur qualité d'image possible. Cette action de formation améliorera significativement la qualité du service rendu par le terminal.

Il est important de noter que l'enrôlement d'un 2ème doigt offre une alternative intéressante lorsque l'utilisateur ne peut plus présenter le 1er doigt (tenue d'un objet, doigt blessé ou sale, dans un gant, etc.).

Il est recommandé d'enrôler comme 1er doigt celui que l'utilisateur présentera le plus spontanément.

Les règles de placement du doigt sont décrites dans la section Annexe 1 : Règles de positionnement du doigt.



Section 2 : Présentation du terminal

Description des interfaces

Introduction

Le document *Guide d'Installation du MorphoAccess® VP Series* décrit précisément chaque interface et la procédure de connexion.

Tous les branchements du terminal décrits ci-après sont de type TBTS (très basse tension de sécurité).

Interface utilisateur (voir figure 6)

Figure 6 : Vue avant du terminal MorphoAccess® VP Series

Les terminaux MorphoAccess® VP proposent une interface homme-machine simple et ergonomique, dédiée au contrôle d'accès basé sur la technologie multimodale de reconnaissance d'empreinte digitale et du réseau veineux :

- (1) un capteur optique de haute qualité pour capturer les données biométriques d'un doigt,
- (2) un voyant LED multicolore,
- (3) un buzzer à tons multiples,
- (4) un lecteur de cartes à puce sans contact en option (MIFARE® et DESFire®).

Interface d'alimentation (voir figure 7)

Le terminal peut être alimenté de deux manières différentes :

- Soit par les bornes d'alimentation +12V VCC/GND (2 fils) : repère (A)
- Soit par l'interface POE (Power Over Ethernet) : soit par le connecteur RJ45 (RJ45/POE) ou par les bornes (B)

Alimentation POE

Le terminal MorphoAccess® VP peut être alimenté, via l'interface Ethernet, en utilisant le mode POE.

- Lorsque le raccordement au réseau est fait par le connecteur RJ45 (RJ45/POE), le terminal accepte aussi bien une alimentation POE sur les broches de données que sur les broches libres.
- Par contre, lorsque le raccordement au réseau est fait par le bornier Ethernet (B), seule l'alimentation POE sur les bornes de données est possible.

Merci de contacter l'administrateur du réseau pour savoir quel mode d'alimentation POE est disponible.

Bouton de réinitialisation (voir figure 8)

Un bouton de réinitialisation (A) permet d'effectuer une brève coupure d'alimentation et donc de forcer un redémarrage complet du terminal (matériel et logiciel).

Ce bouton de réinitialisation se situe sous la trappe amovible inférieure, à proximité du port USB (B).

Interface d'administration (voir figures 7 et 8)

Le terminal dispose de plusieurs ports destinés à son administration :

- Un connecteur Ethernet RJ45 (LAN 10/100 Mbit/s, protocole TCP ou SSL)
- Un bornier Ethernet pour 5 fils (LAN 10/100 Mbit/s, protocole TCP ou SSL)
- Un port USB situé dans la trappe inférieure, destinée à la connexion :
    - D'un adaptateur USB Wi-Fi™,
    - Ou d'une clé mémoire USB, pour effectuer des modifications ponctuelles et limitées.

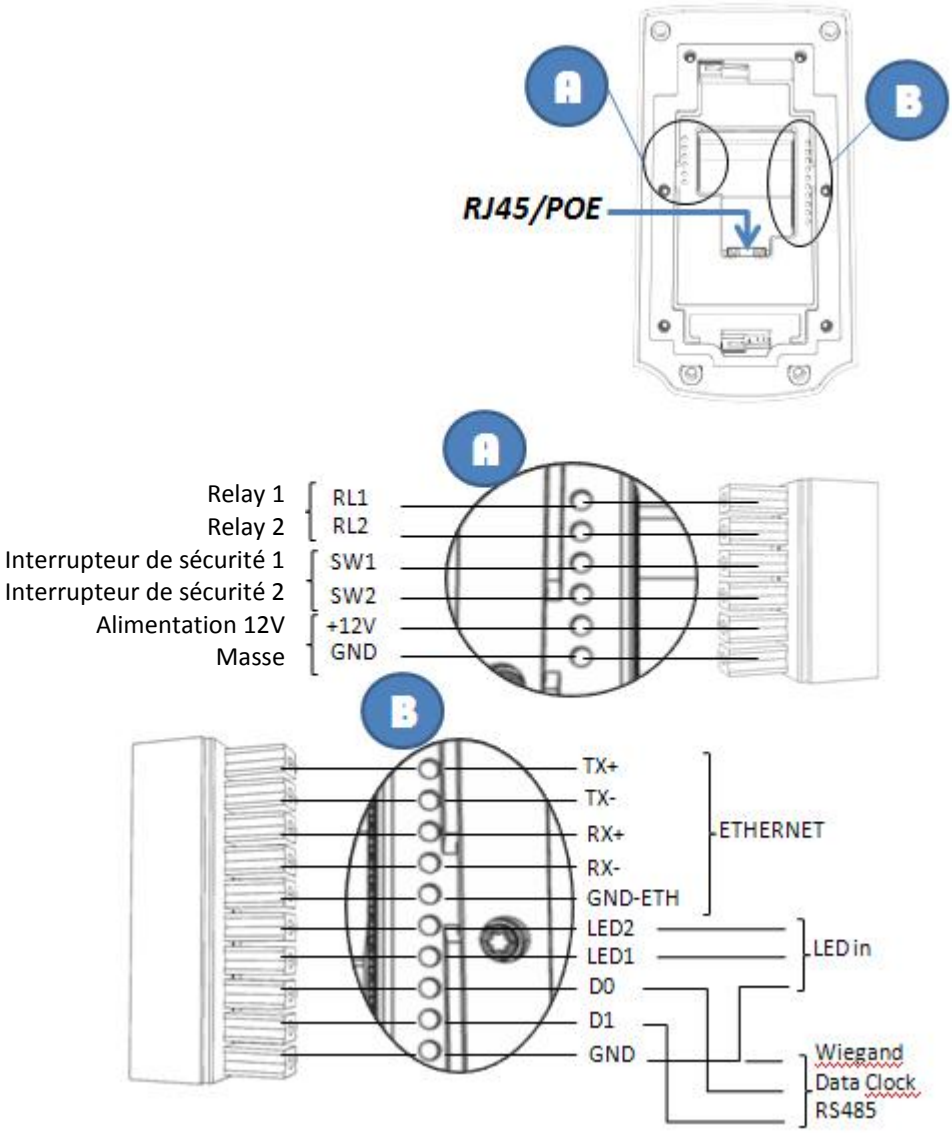


Figure 7 : Vue arrière du terminal MorphoAccess® VP (borniers et connecteurs)

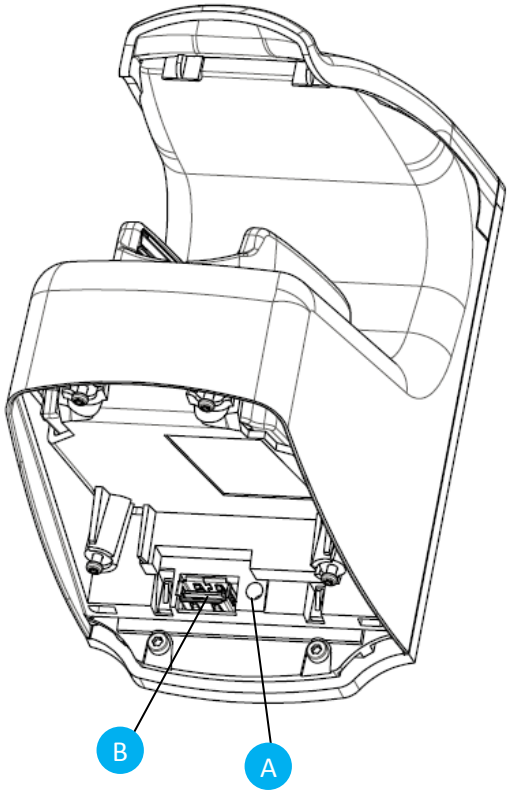


Figure 8 : Face avant du terminal MorphoAccess® VP sans la trappe inférieure

Interface systèmes de contrôle d'accès

Le terminal propose plusieurs interfaces qui facilitent son intégration dans un système de contrôle d'accès global.

Envoi du message de fin de contrôle local

Le terminal peut envoyer un message à un système distant lorsqu'il a terminé ses propres contrôles. Ce message peut être utilisé pour effectuer un simple archivage, ou pour déclencher un processus plus complexe comme effectuer des contrôles de droit d'accès supplémentaires.

Cette fonction est décrite dans la section Envoi du message résultat de contrôle d'accès

Pour cette fonction, le terminal peut utiliser :

- Une liaison Ethernet, soit par le connecteur RJ45 (RJ45/POE) ou par le bornier (B), en utilisant le protocole UDP ou TCP ou SSL
- Une liaison Wi-Fi™, en branchant un adaptateur USB Wi-Fi™ sur le port USB, en utilisant le protocole UDP ou TCP ou SSL
- Le port série (B), en utilisant le protocole Wiegand, DataClock, ou RS485

Il n'est pas possible d'utiliser à la fois la liaison Ethernet et la liaison Wi-Fi™. Par contre, il est possible d'utiliser la liaison série en même temps que la liaison Ethernet ou la liaison Wi-Fi™.

Cette fonction est compatible avec l'administration par lien Ethernet ou Wi-Fi™.

Signaux entrants et contacts de relais

Le terminal MorphoAccess® VP propose les interfaces suivantes :

- deux entrées LED IN (une pour l'accès autorisé, l'autre pour l'accès refusé), pour utilisation dans un système de contrôle d'accès. Cette fonction est décrite dans la section Fonctionnalité LED IN
- un contact de relais (RL1-RL2) pour commander directement un dispositif physique tel qu'une gâche électrique de porte. Cette fonction est décrite dans la section Activation du relais interne.
- un contact de relais (SW1-SW2) reportant l'état des détecteurs anti-arrachement et anti-intrusion. Cette fonction est décrite dans la section Détecteurs anti-intrusion et anti-arrachement.

Utilisation du port USB

Branchement d'une clé mémoire USB

Le port USB type A à l'avant du terminal est dédié à la connexion d'une clé mémoire USB, pour la configuration du terminal à l'aide de scripts de commande ou pour l'upgrade du firmware.

Cette fonction est décrite dans la section Modification paramètres réseau avec clé mémoire USB, et dans les documents suivants :

- MorphoAccess® USB Network Tool User Guide,
- MorphoAccess® USB encoder User Guide.

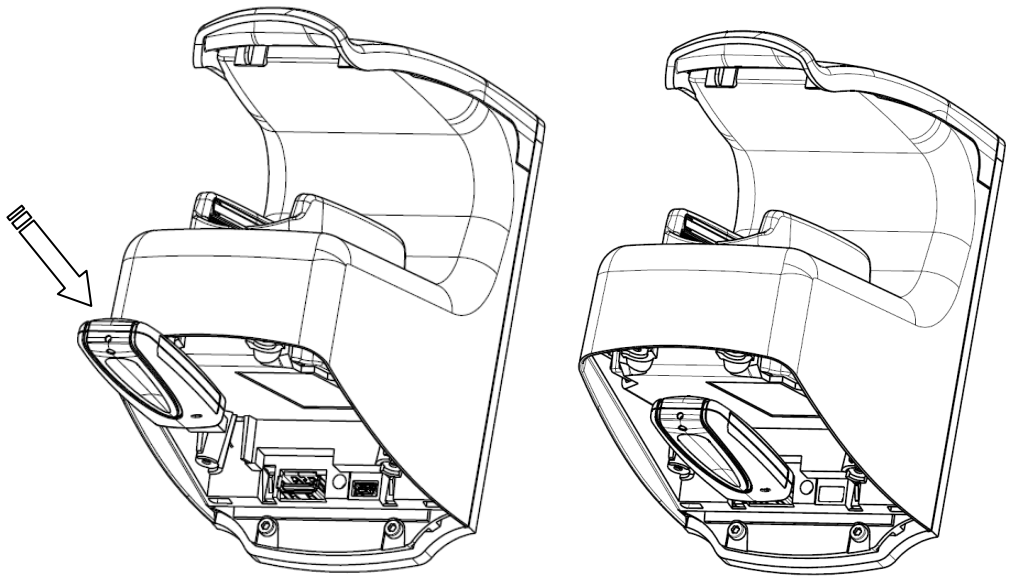


Figure 9 : Port USB frontal du Terminal MorphoAccess® VP avec une clé mémoire USB

Branchement d'un adaptateur USB Wi-Fi™

Le port USB type A à l'avant du terminal peut également servir à la connexion d'un adaptateur Wi-Fi™ USB. Il faut retirer la trappe inférieure pour libérer l'accès à ce port.

L'adaptateur Wi-Fi™ est un accessoire qui peut être commandé sous la référence « PACK MA WI-FI » en même temps que la licence permettant d'activer la fonctionnalité Wi-Fi™ sur le terminal.

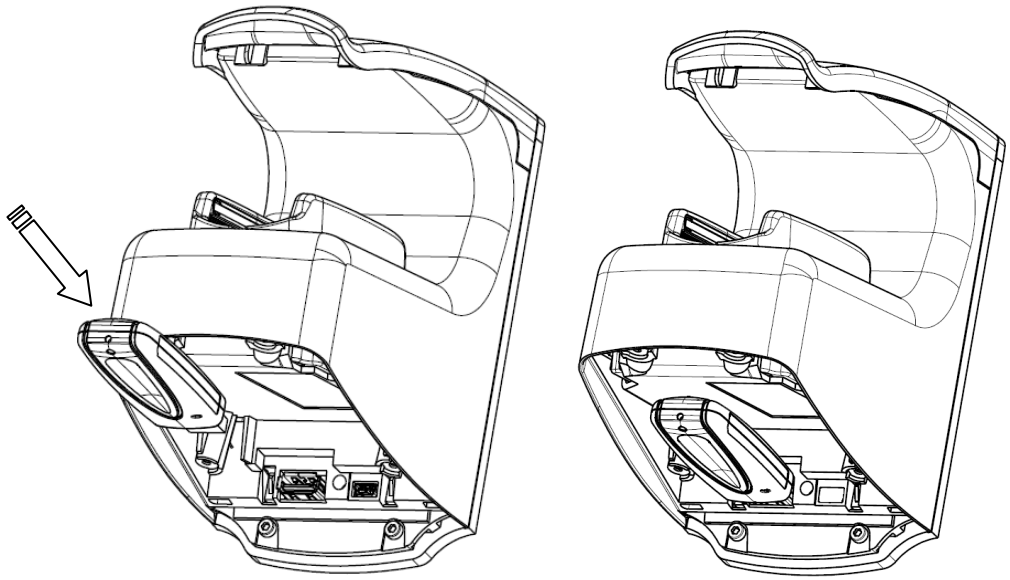
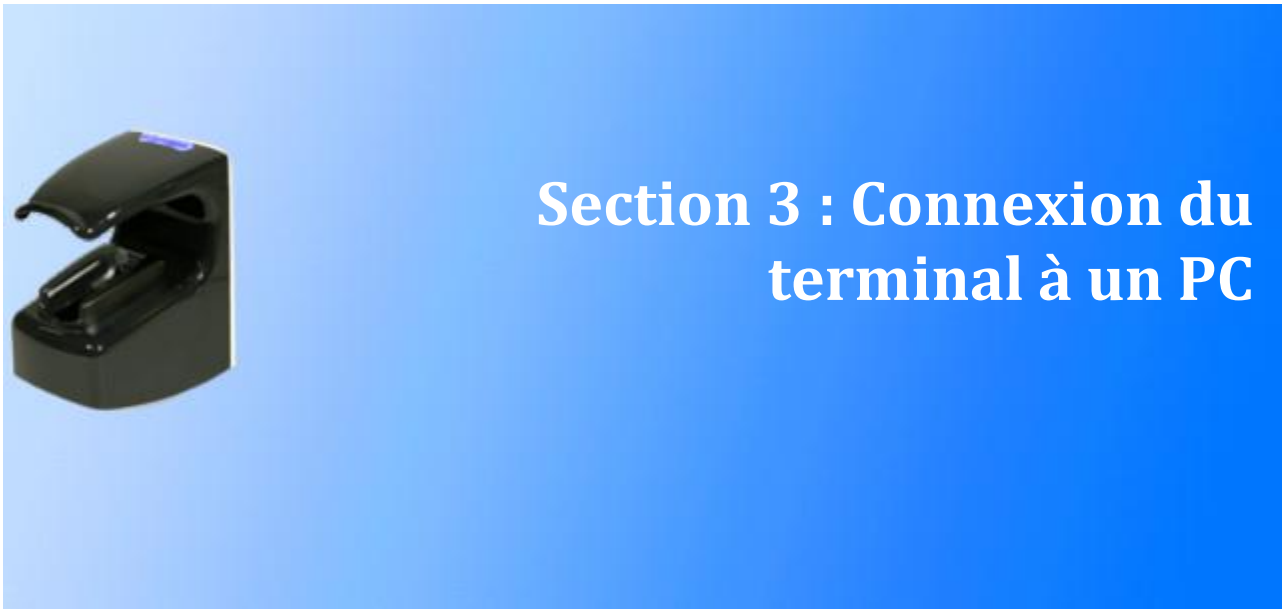


Figure 10 : Port USB arrière du terminal MorphoAccess® VP avec un adaptateur Wi-Fi™



Section 3 : Connexion du terminal à un PC

Généralités

Pourquoi connecter le terminal MorphoAccess® à un PC ?

Le terminal MorphoAccess® VP est conçu pour fonctionner de manière autonome, c'est-à-dire sans être connecté à un système maître. Mais il est parfois nécessaire de le connecter à un PC pour effectuer des tâches comme :

- la configuration du terminal,
- la maintenance du terminal : mise à jour du logiciel embarqué, installation d'une licence,
- la gestion de la base : ajout, modification, suppression d'un utilisateur,
- la gestion du fichier journal : lecture et effacement,
- configurer la liaison Wi-Fi™ avant utilisation.

Méthode de connexion

Le terminal MorphoAccess® peut être connecté à un PC, par un câble Ethernet soit directement, soit à travers un réseau local. Le réseau local pouvant être constitué d'un unique routeur Ethernet.

Une fois connecté physiquement, le terminal MorphoAccess® peut être configuré depuis un PC avec une application comme Morpho Bio Toolbox ou *MATM*.

Un injecteur de courant POE (Power Over Ethernet) est nécessaire si le terminal n'est pas alimenté par les bornes 12VDC/GND.

Initialisation des paramètres réseau

Les paramètres de connexion du terminal MorphoAccess® sont les suivants :

Affectation adresse IP	Donnée	Valeur usine
Fixe (par défaut)	Adresse IP du terminal	134.1.32.214
	Adresse IP de la passerelle	134.1.6.20
	Masque de sous-réseau	255.255.240.0
Dynamique (DHCP)	Nom d'hôte (host name)	MA<Numéro de série>

S'il n'est pas possible d'utiliser les paramètres réseau par défaut du terminal, le moyen le plus rapide de les changer est d'utiliser une clé mémoire USB.

La procédure est décrite dans le paragraphe Modification paramètres réseau avec clé mémoire USB.

Connexion Ethernet en Point à Point

Un terminal MorphoAccess® peut être connecté directement à un PC par un simple câble Ethernet.

Ceci, avec les restrictions suivantes :

- Si le port Ethernet du PC ne supporte pas la fonction Auto-MDIX, alors il faudra utiliser impérativement un câble Ethernet croisé. S'il n'y a pas de câble croisé disponible, il est possible d'utiliser un routeur Ethernet (voir section suivante)
- Si le PC à utiliser est connecté sur un réseau local, il faudra, soit le débrancher, soit l'équiper d'une deuxième carte d'interface réseau qui sera dédiée à la connexion du terminal. Et il sera peut être nécessaire de modifier les paramètres réseau : veuillez contacter votre administrateur réseau pour définir la meilleure solution.

Figure 11 : Connexion Ethernet directe en point à point

Connexion Ethernet à travers un routeur Ethernet

Un terminal MorphoAccess® peut être connecté à un PC par l'intermédiaire d'un routeur Ethernet (switch). Cette solution s'impose lorsqu'il n'y a pas de câble croisé Ethernet disponible. Mais il faut cette fois deux câbles Ethernet droits et un routeur.

ATTENTION: un HUB Ethernet ne permet pas la connexion entre deux de ses ports. Il est vraiment indispensable d'utiliser un routeur Ethernet (switch).

Figure 12 : Connexion à travers un routeur Ethernet

Connexion à travers un réseau local

Description

Le terminal MorphoAccess® peut être connecté à un PC à travers un réseau local.

Le PC désigne le terminal MorphoAccess® auquel il veut se connecter par son adresse IP ou par son nom d'hôte (lorsqu'il est possible de la déclarer dans le serveur DNS du réseau). L'adresse IP du terminal est soit fixe, soit attribuée dynamiquement par le serveur DHCP du réseau.

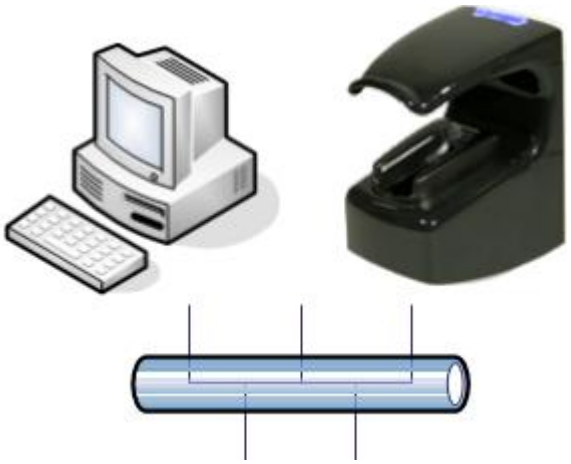


Figure 13 : Connexion à travers un réseau local (LAN)

Il est fortement recommandé de connecter le terminal MorphoAccess® à un réseau dédié pour réduire le risque d'accès frauduleux à la configuration du terminal. Merci de contacter l'administrateur du réseau pour plus d'information à propos de la stratégie de sécurité du réseau local.

Avant de connecter le terminal MorphoAccess® à un réseau local, il faut d'abord lui indiquer la valeur des paramètres réseau à utiliser. Ces valeurs sont à fournir et/ou approuver par l'administrateur du réseau.

Réseau local avec serveur DNS

Lorsque le réseau local comprend un serveur DNS, il possible de désigner le terminal MorphoAccess® par son nom d'hôte à la place de son adresse IP.

Mais pour cela, il faut impérativement déclarer le nom d'hôte du terminal MorphoAccess® dans la base du serveur DNS. Sinon toute demande de connexion avec le nom d'hôte échouera systématiquement. Merci de contacter l'administrateur du réseau pour réaliser cette opération dans le serveur DNS.

La possibilité de demander une connexion en utilisant un nom d'hôte est particulièrement intéressante lorsque le mode DHCP est activé. En effet, dans ce cas,

l'adresse IP du terminal MorphoAccess® est susceptible de changer à chaque mise sous tension.

Réseau local sans serveur DNS

Cette section concerne le cas d'un réseau local sans serveur DNS, mais également le cas d'un réseau local avec un serveur DNS sans possibilité d'ajouter le nom du terminal.

Dans ce cas, l'établissement d'une session TCP par le PC en spécifiant le nom du terminal ne pourra pas aboutir. Il n'y a pas d'autre possibilité que d'utiliser l'adresse IP du terminal.

Pour une utilisation normale (hors maintenance ponctuelle), il est donc déconseillé d'activer le mode DHCP dans le terminal. En effet quand ce mode est actif, l'adresse IP du terminal peut changer à chaque mise sous tension.

Adresse IP fixe (DHCP inactif)

C'est le moyen le plus simple de connecter un terminal MorphoAccess® à un réseau local : l'adresse IP du terminal reste la même, y compris après un redémarrage. Le PC utilisé à juste besoin de connaitre l'adresse IP du terminal pour s'y connecter.

L'adresse IP du terminal MorphoAccess® doit être réservée dans le routeur par l'administrateur réseau. C'est également, l'administrateur réseau qui doit fournir et/ou approuver la valeur des paramètres réseau du terminal. C'est-à-dire :

- L'adresse IP du terminal MorphoAccess®,
- L'adresse IP de la passerelle du sous réseau,
- La valeur du masque du sous-réseau.

Attention : si le terminal MorphoAccess® utilise une adresse IP déjà utilisée dans le réseau, la connexion à ce terminal sera instable.

Adresse IP dynamique (DHCP actif)

Lorsque le mode DHCP est activé dans le terminal, à chaque démarrage le terminal demande une adresse IP au routeur du réseau. Cette adresse n'est pas obligatoirement la même à chaque fois.

Merci de contacter votre administrateur réseau pour savoir si le mode DHCP est supporté par le réseau.

Modification paramètres réseau avec clé mémoire USB

Les paramètres de connexion au réseau peuvent être initialisés (et changés), en utilisant une clé mémoire USB. Le terminal n'a pas besoin d'être connecté au PC. Cette opération nécessite une application PC dédiée: USB Network Configuration Tool et une clé mémoire USB standard (formatée FAT32, et capacité maximale de 8 Go).

Ceci est particulièrement utile pour les terminaux MorphoAccess® sans clavier et sans écran, mais fonctionne aussi avec les terminaux dotés d'un clavier et un écran.

La méthode est détaillée dans les paragraphes ci-dessous, et dans le document *USB Network Tool User Guide*.

Etape 1 : Génération du fichier de commande sur la clé mémoire USB

Lancer l'application *USB Network Configuration Tool* sur un PC : la fenêtre ci-dessous est affichée sur l'écran du PC.

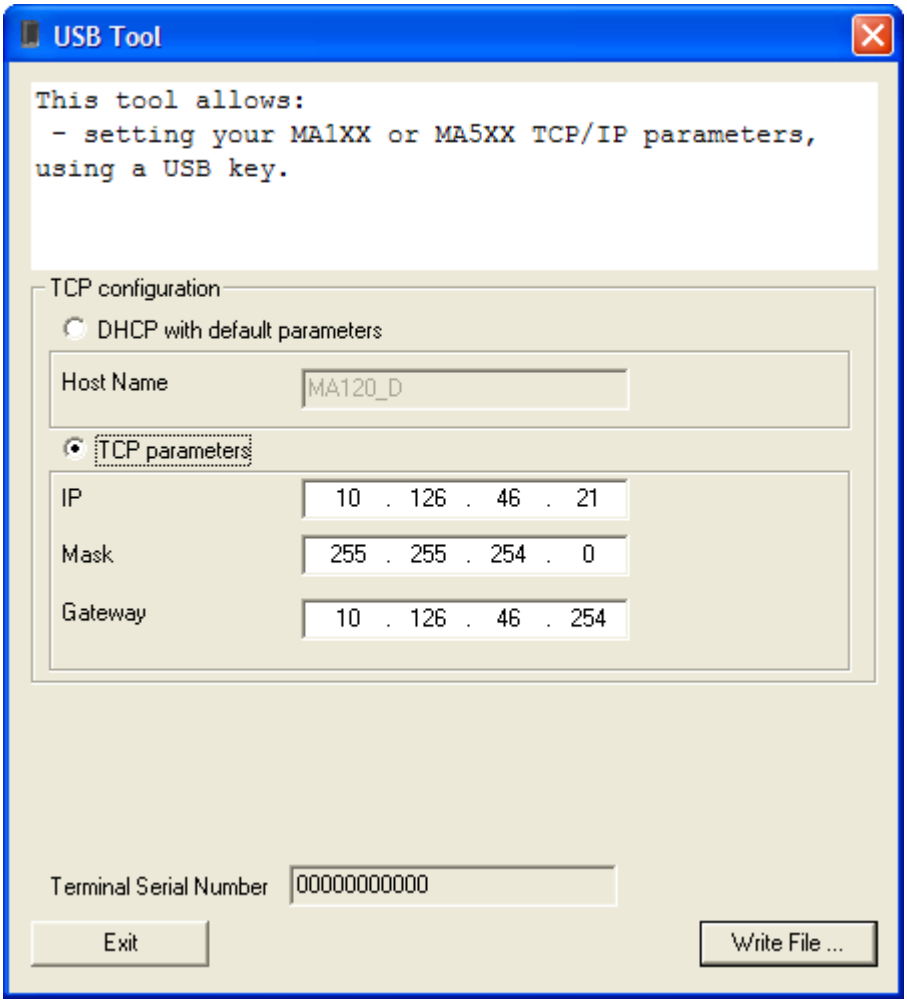


Figure 14 : Fenêtre principale de l'application USB Network Configuration Tool

Si ce n'est pas déjà fait insérer la clé mémoire USB dans un port USB libre du PC.

En premier lieu, choisir si le mode DHCP doit être activé (adresse IP dynamique) ou non (adresse IP fixe).

- Si le mode DHCP doit être activé, indiquer le nom d'hôte du terminal, choisi en accord avec l'administrateur du réseau local.
- Si le mode DHCP ne doit pas être activé, indiquer les valeurs des paramètres ci-dessous, telle qu'elles ont été communiqués par l'administrateur du réseau.

Le champ « numéro de série » n'est utile que lorsque le protocole SSL est activé sur le terminal.

Quand tous les champs ont été remplis avec les données approuvées par l'administrateur du réseau, cliquer sur le bouton « *Write File* ». Sélectionner ensuite le répertoire racine de la clé mémoire USB.

Après validation du répertoire, l'application génère un fichier de commande et un fichier d'adresse.

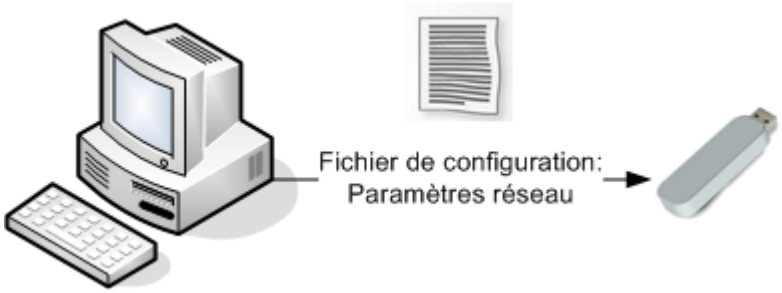


Figure 15 : Enregistrement des données sur une clé mémoire USB

Etape 2: appliquer les changements au terminal

Retirer la trappe inférieure du terminal MorphoAccess® VP, pour libérer l'accès au port USB du terminal.

Après s'être assuré que le terminal est bien sous tension, insérer la clé mémoire USB, utilisée lors de l'étape précédente, dans le port USB type A du terminal.

Le terminal exécute alors un processus de plusieurs secondes, dont la progression est indiquée par des signaux sonores et lumineux (voir section IHM Lumineuse et sonore), et qui se termine par la demande de retrait de la clé mémoire USB. Après le retrait de celle-ci, le terminal redémarre pour appliquer les nouvelles valeurs de paramètres.

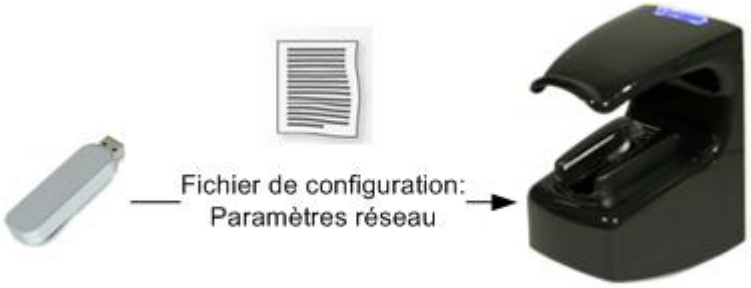


Figure 16 : Application du fichier de configuration au terminal

Le terminal est alors prêt à être connecté au réseau.

Configuration du réseau Wi-Fi™

Pré-requis

La connexion Wi-Fi™ est disponible dans les conditions obligatoires suivantes :

- une clé Wi-Fi™ Morpho est branchée sur le port USB du terminal. La procédure d'installation est décrite dans le document Guide d'installation du MorphoAccess® VP Series,
- une licence Wi-Fi™ (dédiée à ce terminal) est chargée dans le terminal (cf. paragraphe « Gestion des licences du terminal MorphoAccess® »),
- le terminal n'est pas connecté à un réseau avec un câble Ethernet : la connexion Wi-Fi™ et la connexion par câble Ethernet sont exclusives l'une de l'autre.

Redémarrer le terminal en appuyant sur le bouton de réinitialisation, après le téléchargement de la licence Wi-Fi™ et l'installation de la clé Wi-Fi™ (consulter le paragraphe Interface d'alimentation, pour plus d'informations sur le bouton de réinitialisation).

NOTE : La clé Wi-Fi™ et la licence peuvent être toutes deux commandées sous la référence « PACK MA WI-FI ».

Configuration

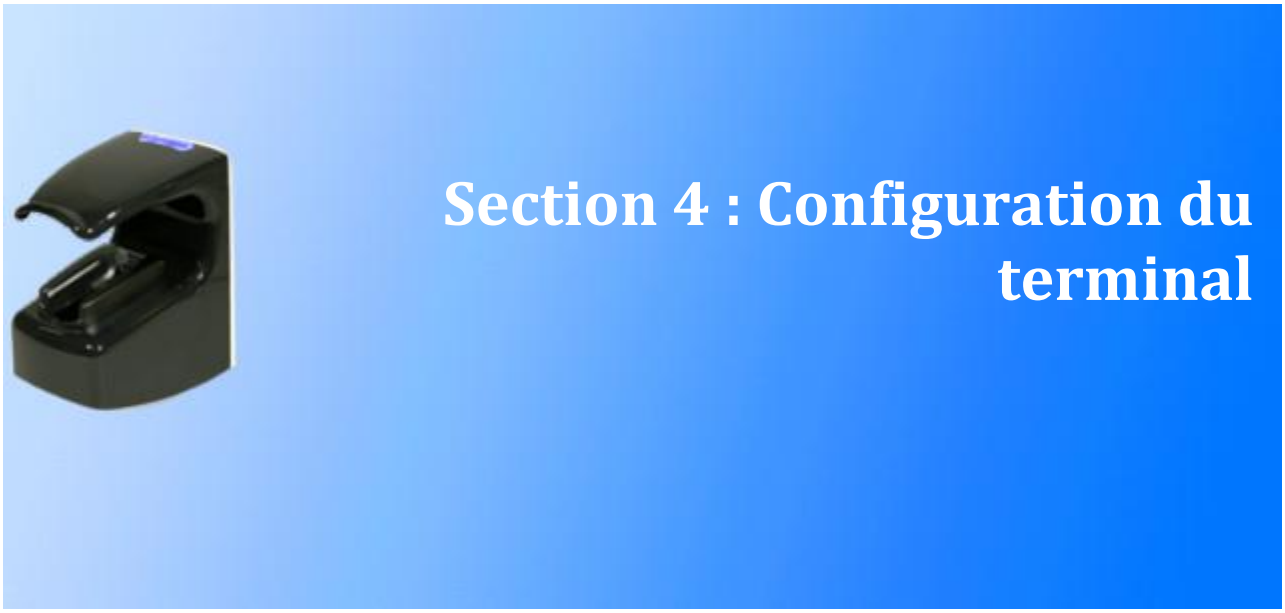
La configuration du terminal pour la connexion à un réseau Wi-Fi™ est décrite dans le chapitre 15 du document MorphoAccess® Enrollment station User Guide.

Résolution de problème

Si le terminal est configuré pour utiliser la connexion Wi-Fi™ avec la clé Wi-Fi™ branchée et qu'aucune licence Wi-Fi™ n'est présente, le terminal émet une lumière clignotante rouge d'une seconde et une tonalité basse et brève.

Pour résoudre ce problème, débrancher la clé Wi-Fi™ et redémarrer le terminal. Pour redémarrer le terminal, utiliser le bouton de réinitialisation situé sur la face avant du terminal (voir section Interface d'alimentation, pour plus d'informations sur le bouton de réinitialisation).

Les paramètres Wi-Fi™ sont décrits dans le paragraphe correspondant du document MorphoAccess® Parameters Guide.



Section 4 : Configuration du terminal

Paramètres de configuration du MorphoAccess®

Présentation

Le nom et la valeur des paramètres d'un terminal MorphoAccess® (également appelés « clés de configuration ») sont répartis dans plusieurs fichiers, eux-mêmes découpés en sections, afin de les regrouper par affinité.

Par exemple, un fichier nommé « app.cfg » contient tous les paramètres définissant les principaux réglages de l'application (de contrôle d'accès), et la section « bio ctrl » regroupe les réglages du contrôle biométrique.

Le nom complet de la clé de configuration comprend le nom du fichier et le nom de la section, soit : « nom de fichier/nom de section/nom de clé ». Exemple : « app/bio ctrl/nb attemps »

Toutes les clés de configuration sont décrites dans le document *MorphoAccess® Parameters Guide*.

Modification de la valeur d'un paramètre

Un paramètre de configuration peut être modifié de deux manières :

- via une connexion Ethernet ou Wi-Fi™, avec une application client fonctionnant sur le système hôte, comme Morpho Bio Toolbox ou *MATM.exe*
- via une clé mémoire USB contenant un script préparé sur un PC (pour plus d'informations, consulter le document *MorphoAccess® USB Key Encoder User Guide*).

Configuration d'un terminal MorphoAccess® connecté

Introduction

Un terminal MorphoAccess® peut être administré par un PC si celui-ci est connecté au terminal, en utilisant une application comme : Morpho Bio Toolbox, MATM, MorphoEnroll.

Les opérations pouvant être réalisées à distance sont principalement :

- Ajout d'un utilisateur (création d'un enregistrement biométrique),
- Suppression d'un utilisateur (d'un enregistrement biométrique),
- Lecture d'une clé de configuration,
- Modification de la valeur d'une clé de configuration,
- Lecture du journal des demandes d'accès (fichier Log),
- Renouvellement des clés d'authentification des cartes sans contact,
- Mise à jour du micro logiciel,
- Ajout d'une licence.

Le terminal MorphoAccess® agit en tant que serveur TCP/IP dans l'attente d'une commande émise par l'application PC, qui elle, agit comme un client TCP/IP.

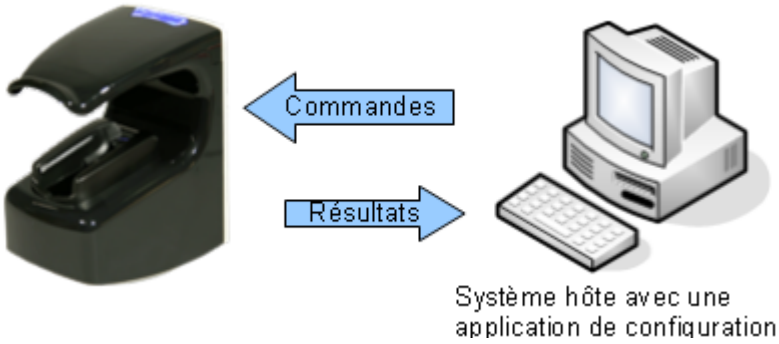


Figure 17 : Configuration d'un terminal MorphoAccess® par un système hôte

Les commandes acceptées par le terminal MorphoAccess® sont décrites dans le document *MorphoAccess® Host System Interface Specifications*.

Réglage de la date et de l'heure

La date et l'heure du terminal peuvent être initialisées par un système hôte distant à l'aide d'une application telle que l'outil « Morpho Bio Toolbox » (onglet « Configuration », bouton « Régler la date et l'heure ») décrit ci-dessous.

Application PC « Morpho Bio Toolbox »

L'application « *Morpho Bio Toolbox* » peut être utilisée pour lire et modifier la valeur de tous les paramètres de configuration du terminal MorphoAccess®.

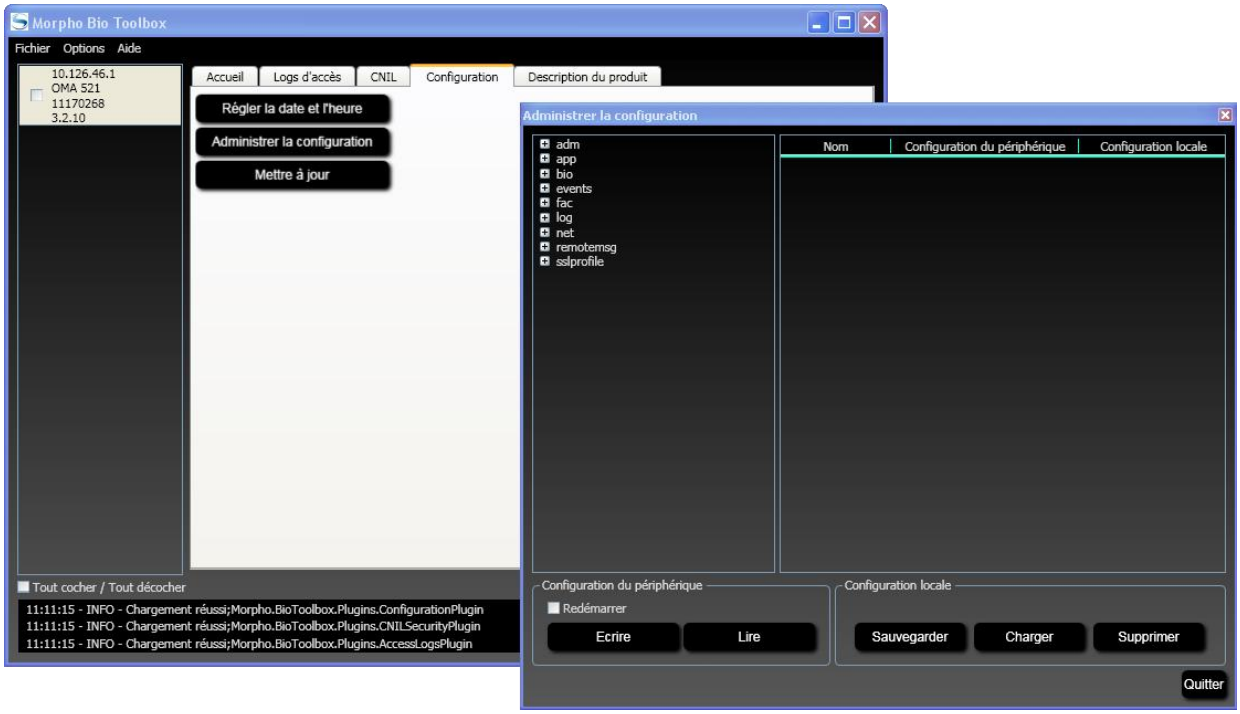


Figure 18 : Fenêtre de configuration de l'outil Morpho Bio Toolbox

Pour plus d'informations sur cette application, veuillez consulter le guide de l'utilisateur disponible dans le menu « Aide » de l'application Morpho Bio Toolbox

Application PC MATM

MATM est une autre application PC qui permet la lecture et la modification des paramètres de configuration du terminal MorphoAccess®.

Par rapport à Morpho Bio Toolbox, cette application permet en plus d'effectuer la configuration du terminal en Wi-Fi™, et l'activation du protocole SSL.

La procédure de modification d'une clé de configuration avec MATM est décrite dans le document MorphoAccess® Terminal Management User Guide.

Sécurisation SSL

La liaison TCP utilisée pour gérer le terminal peut être sécurisée à l'aide du protocole SSL. Pour plus de détails, consulter le document SSL Solution for MorphoAccess®.

Mise à niveau du logiciel embarqué

Quand c'est nécessaire, il est possible de mettre à niveau le micro logiciel d'un terminal MorphoAccess® depuis un PC, en utilisant une connexion IP (Ethernet ou Wi-Fi™), ou bien une clé mémoire USB.

La dernière version du micro logiciel disponible pour le terminal MorphoAccess® peut être obtenue sur un CD/ROM auprès du service après vente, ou bien téléchargé depuis le site Web de Morpho dédié au terminaux biométriques :

http://www.biometric-terminals.com/

Un identifiant (login) et un mot de passe (password) sont nécessaires : ils peuvent être obtenus en contactant l'assistance à l'adresse ci-dessous.

hotline.biometrics@t.my-technicalsupport.com

Pour plus d'informations sur les procédures de mise à jour du logiciel embarqué, veuillez consulter le document *MorphoAccess® Firmware Upgrade Guide*.

Gestion de la base du terminal MorphoAccess®

Généralités

La gestion de la base interne du terminal MorphoAccess® peut être effectuée à distance par une station d'enrôlement, composée d'un PC et de l'application MorphoEnroll, ou une application développée avec la librairie Active_MACI.

La mise à jour de la base (ajout/suppression d'utilisateur) peut se faire par l'intermédiaire d'une clé mémoire USB, comme décrit dans le document MorphoAccess® USB encoder User Guide.

Ajout d'un utilisateur à la base

L'ajout d'un utilisateur à la base revient à ajouter un enregistrement avec les données biométriques de deux des doigts de l'utilisateur, et un identifiant unique.

L'application MorphoEnroll effectue directement l'enrôlement de l'utilisateur sur le terminal MorphoAccess® sans gérer de base sur le PC.

Suppression d'un utilisateur de la base

La suppression d'un utilisateur revient à effacer l'enregistrement de la base du terminal MorphoAccess®.

L'application MorphoEnroll supprime directement l'utilisateur dans le terminal MorphoAccess® sans gérer de base sur le PC.

Taille de la base

La base du terminal MorphoAccess® VP peut stocker 5.000 utilisateurs, ou bien 10.000 utilisateurs avec une licence MA_10K_USERS. Pour chaque utilisateur, le terminal conserve les données biométriques de deux doigts.

Gestion des licences du terminal MorphoAccess®

Définition d'une licence

L'installation d'une licence débloque une fonctionnalité supplémentaire du terminal.

Le terminal MorphoAccess® VP peut recevoir les licences suivantes :

- MA _10K_USERS,
- MA_WIFI.

La fonction de chacune de ces licences est détaillée dans les paragraphes suivants.

Licence MA_10K_USERS

Par défaut, la capacité maximale de la base d'un MorphoAccess® VP est de 5.000 utilisateurs (chaque enregistrement comprenant les données de deux doigts).

La licence MA_10K_USERS permet d'étendre la capacité maximale de la base à 10.000 utilisateurs (chaque enregistrement comprenant les données de deux doigts).

Attention : l'extension de la capacité de la base n'est pas dynamique. L'installation de la licence autorise la création d'une base de plus grande capacité, mais elle ne modifie pas la capacité maximale de la base existante. Celle-ci doit donc être effacée, puis recréée (avec la nouvelle taille) pour que l'extension de capacité soit effective.

Licence MA_WIFI

La licence MA_WIFI débloque l'utilisation d'une liaison Wi-Fi™ (WLAN) en remplacement de la liaison Ethernet.

Attention : La licence seule ne suffit pas, un adaptateur Wi-Fi™ USB compatible avec le terminal MorphoAccess® est nécessaire. L'adaptateur et la licence peuvent être tous deux commandés sous la référence « PACK MA WI-FI ».

Obtenir une licence

Un compte sur le notre site web dédié aux terminaux biométriques permet d'obtenir une licence par messagerie : voir rubrique « Licence Generator ». Si vous n'avez pas de compte, veuillez contacter notre service d'assistance.

La licence est fournie dans un fichier dédié à un seul terminal. Chaque fichier de licence est généré pour un numéro de série unique, et celui-ci est vérifié par l'outil d'installation de licence, lors de l'ajout de la licence au terminal. Le fichier ne doit être modifié.

Consulter les licences installées

Une liaison Ethernet (ou Wi-Fi™), et l'application *Licence Manager* sont nécessaires pour consulter les licences installées et pour ajouter une licence. L'application peut être téléchargée depuis le site web dédié à nos terminaux biométriques (voir la section assistance).

Lancer l'application *Licence Manager*, faire un clic droit dans la fenêtre principale, et choisir l'opération « Select a MA2G », puis saisir l'adresse IP du terminal.

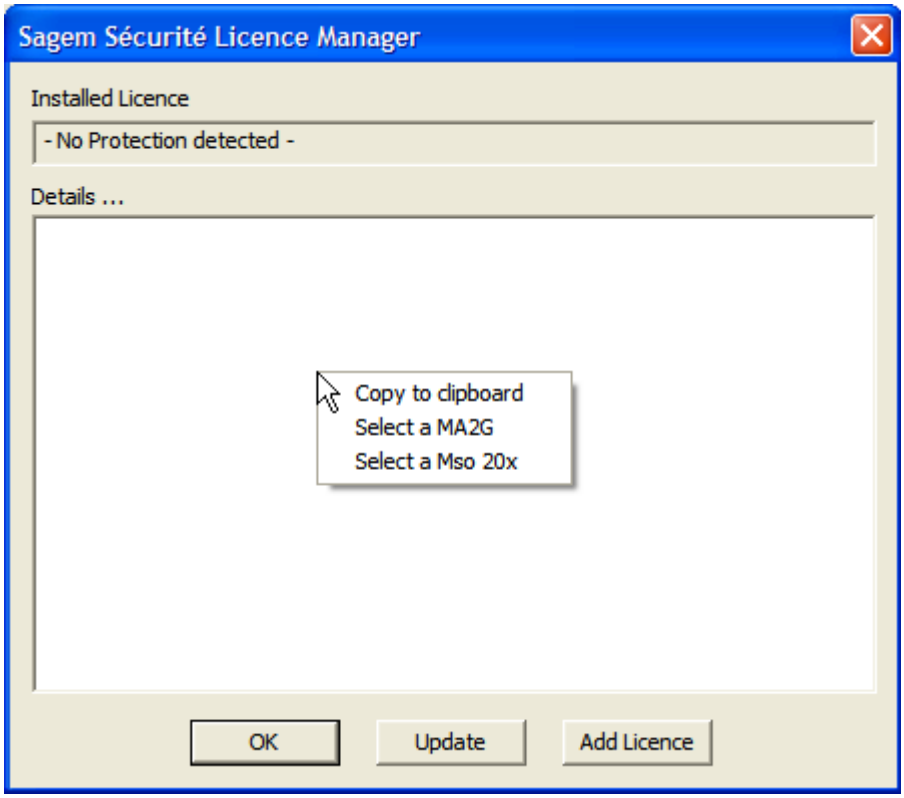


Figure 19 : Licence Manager, déclaration d'un terminal MorphoAccess®

Saisir l'adresse IP du terminal dans la fenêtre qui s'ouvre.

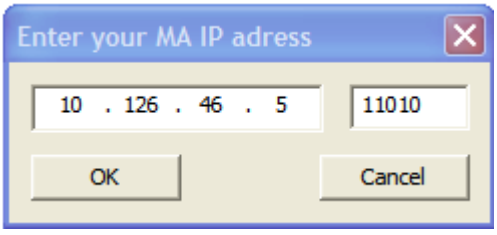


Figure 20 : Licence Manager, saisie adresse IP d'un terminal MorphoAccess®

Les licences présentes dans le terminal MorphoAccess® sont alors affichées dans la ligne « licence in hardware » de la fenêtre principale.

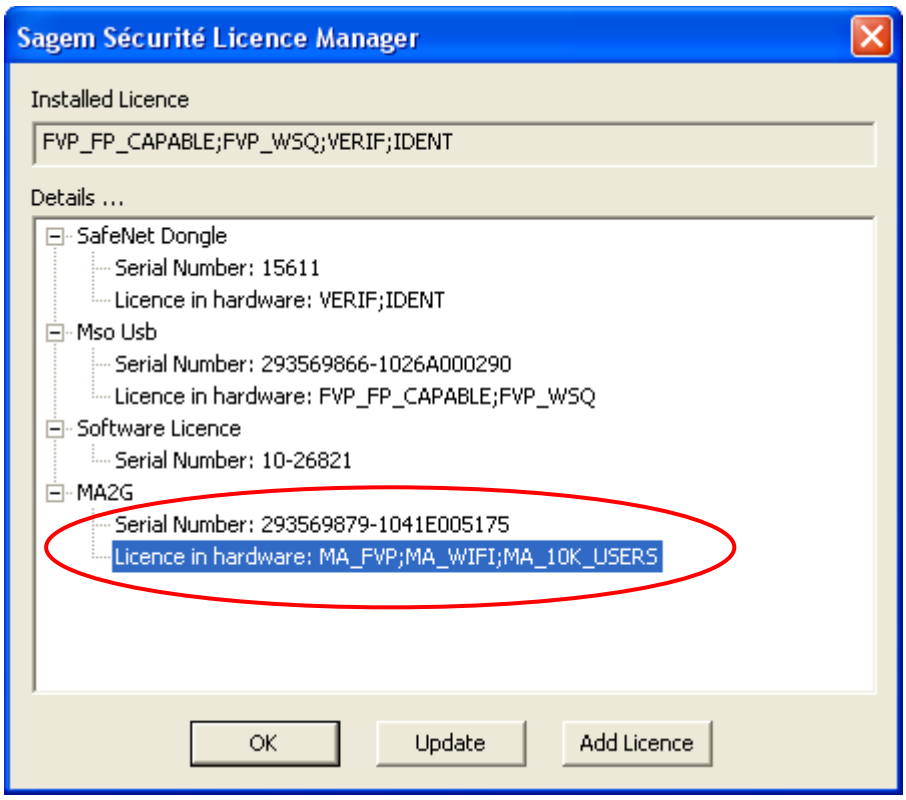


Figure 21 : Licences installées dans un terminal MorphoAccess®

Pour plus d'information sur l'outil de gestion de licences (outil PC *Licence Manager*), merci de consulter le document *MorphoAccess® Terminal Licence Management*.

Installer une nouvelle licence

Pour installer une nouvelle licence, suivre la procédure suivante :

- Lancer l'application « Licence Manager », et déclarer le terminal MorphoAccess® comme indiqué dans la section Consulter les licences installées ci-dessus.
- Une fois obtenu, copier le fichier licence sur le PC
- Relancer l'application « Licence Manager », déclarer le terminal MorphoAccess® comme précédemment, cliquer sur le bouton "Add licence", puis sur le bouton "Browse…" pour sélectionner le fichier licence (.LIC).
- Une fenêtre spécifique s'ouvre ensuite pour indiquer le succès (ou l'échec) du chargement.
- La fenêtre principale indique alors la présence de la nouvelle licence.

Le terminal doit être redémarré pour que les fonctions débloquées par la nouvelle licence soient activées.

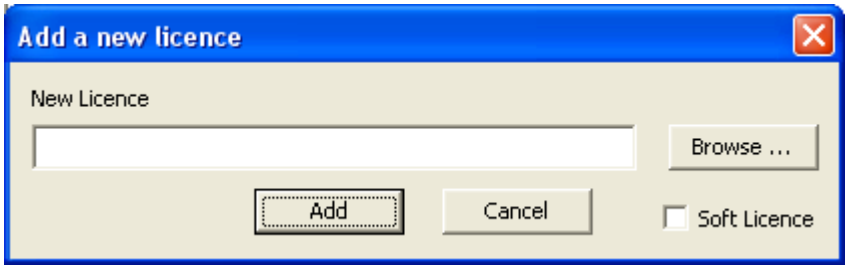
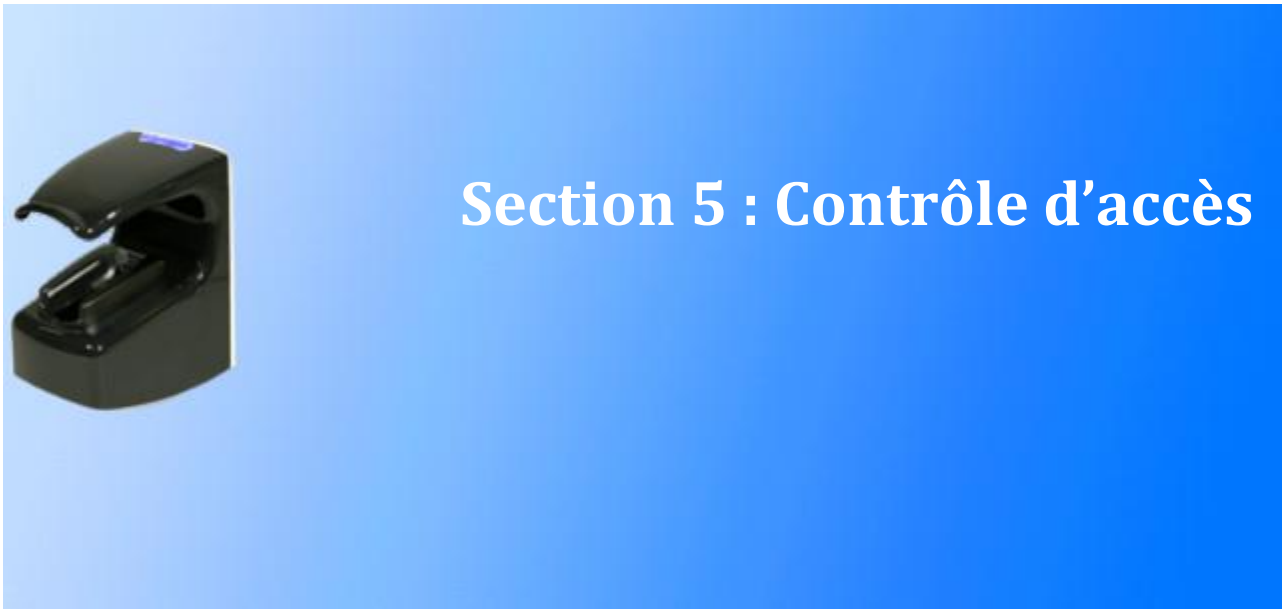


Figure 22 : Ajout d'une licence dans un terminal MorphoAccess®

Pour plus d'information sur l'outil de gestion de licences (outil PC *Licence Manager*), merci de consulter le document *MorphoAccess® Terminal Licence Management*.


Section 5 : Contrôle d'accès

Présentation du contrôle d'accès

Système de contrôle d'accès type

L'architecture d'un système de contrôle d'accès typique comprend :

- un terminal (MorphoAccess®) par zone à protéger,
- Un utilitaire de gestion des utilisateurs (type MorphoEnroll),
- un contrôleur d'accès central, qui effectue les contrôles complémentaires, et qui émet la commande physique autorisant l'accès (ouverture de porte).

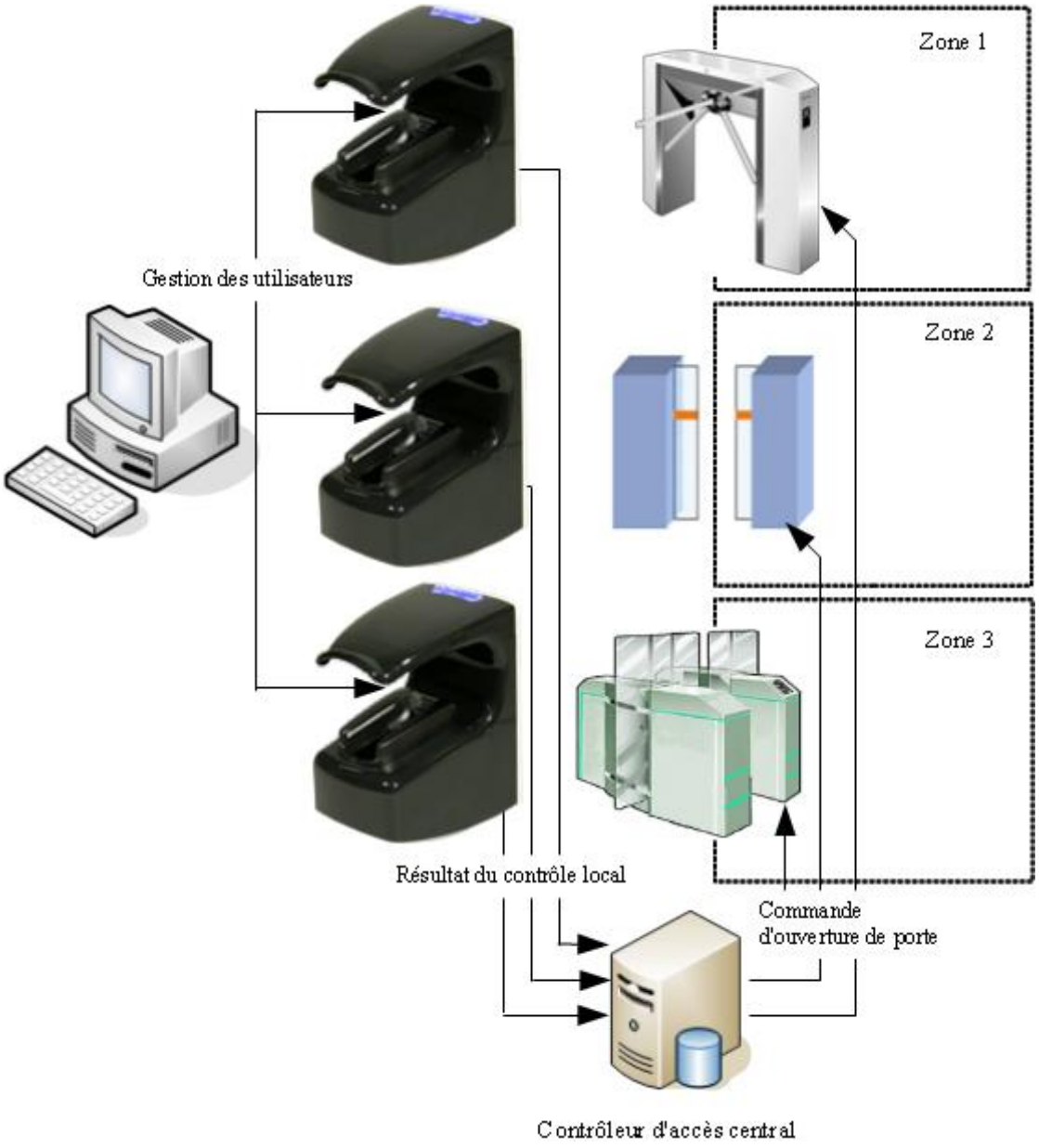


Figure 23 : Architecture typique d'un système de contrôle d'accès

Fonctionnement d'un système de contrôle d'accès typique

1. Tout utilisateur autorisé doit être enregistré. C'est-à-dire que pour chaque utilisateur, un enregistrement comprenant un identifiant unique et les données biométriques de deux de ses doigts, est créé.
2. Quand un utilisateur demande l'accès à une zone protégée, le terminal effectue une vérification des droits d'accès (avec contrôle biométrique).
3. Si le résultat de la vérification est positif (accès autorisé), un message est envoyé au contrôleur d'accès central pour que celui-ci effectue ses propres vérifications.
4. Si l'utilisateur est autorisé à accéder à la zone protégée, le contrôleur d'accès central retourne un message « accès autorisé » au terminal, et une commande au contrôleur de porte.

Modes de fonctionnement du terminal MorphoAccess®

Mode autonome ou mode esclave

Le terminal propose deux modes de fonctionnement mutuellement exclusifs :

- un mode autonome, où le terminal exécute un programme de contrôle d'accès qui peut prendre la décision d'accès seul, ou avec l'autorisation d'un contrôleur d'accès central. Ce mode est détaillé dans la section ci-dessous.
- un mode Proxy (esclave), où un système distant exécute une application de contrôle d'accès qui utilise les fonctions de haut niveau du terminal. Ce mode est détaillé dans la section 9 : Mode Proxy (mode esclave).

Mode autonome : Identification et/ou authentification

Le mode autonome du terminal MorphoAccess® comprend deux processus distincts, qui peuvent être utilisés séparément ou ensemble :

- Un processus « identification », qui est lancé par la détection d'un doigt sur le capteur biométrique. Ce mode est décrit dans la Section 6 : Contrôle d'accès par Identification
- Un mode « authentification », qui est lancé par la détection d'une carte utilisateur, l'étape suivante étant le placement d'un doigt sur le capteur biométrique. Ce mode présente plusieurs variantes suivant l'emplacement des données biométriques et le niveau de sécurité souhaité. Ce mode est décrit dans la Section 7 : Contrôle d'accès par authentification.

L'identification et l'authentification peuvent être activées simultanément, comme décrit dans la Section 8 : Mode Multi-facteurs).

Comment choisir le processus de contrôle d'accès

Le schéma ci-dessous indique les différents processus disponibles, ainsi que les clés de configuration correspondantes.

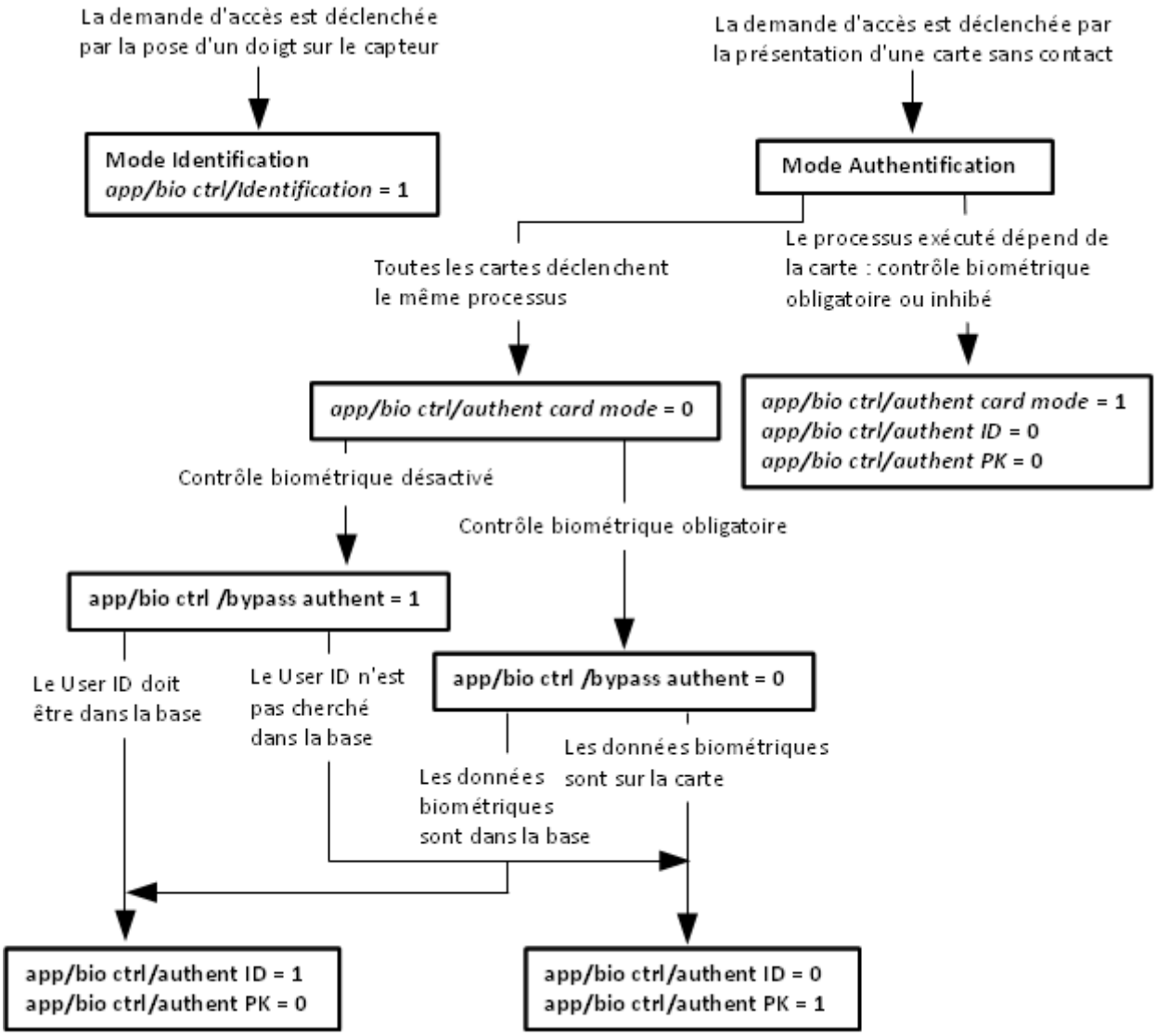


Figure 24: Synthèse des modes de reconnaissance

L'identification et l'authentification peuvent être activées simultanément, comme décrit dans la Section 8 : Mode Multi-facteurs).

.

Résultat du contrôle d'accès

Information de l'utilisateur

Le terminal MorphoAccess® communique le résultat de la vérification des droits d'accès par un signal lumineux et sonore. Ces signaux sont décrits dans la Section 12 : Interface homme-machine MorphoAccess® VP Series.

Par exemple :

- Lorsque l'accès est autorisé, le terminal émet un éclairage vert au niveau de sa LED d'état, et un bip aigu.
- Lorsque l'accès est refusé, le terminal émet un éclairage rouge au niveau de sa LED d'état, et un bip grave.

Information pour l'administrateur

Le terminal MorphoAccess® crée un enregistrement pour chaque demande d'accès, dans un fichier journal interne. Cet enregistrement contient la date et l'heure, l'identifiant de l'utilisateur (si disponible) et le résultat donné à la demande d'accès. Cette fonction est décrite dans la section Journalisation des demandes d'accès (log).

Intégration dans un système de contrôle d'accès

A la fin du contrôle local de droits d'accès, le terminal MorphoAccess® terminal peut:

- Envoyer à un système distant, un message contenant les données relatives à la demande d'accès. Cette fonction est détaillée dans la section Envoi du message résultat de contrôle d'accès.
- attendre (ou non) la réponse du système distant, après l'envoi du message, avant de donner la réponse finale au demandeur d'accès. Cette fonction est détaillée dans la section Fonctionnalité LED IN.
- Activer son relais interne (uniquement si l'accès est autorisé). Cette fonction est détaillée dans la section Activation du relais interne.

Le format des messages (contenant l'identifiant de l'utilisateur) envoyés au système distant sont décrits dans le document *MorphoAccess® Remote Messages Specification*.

Accès autorisé

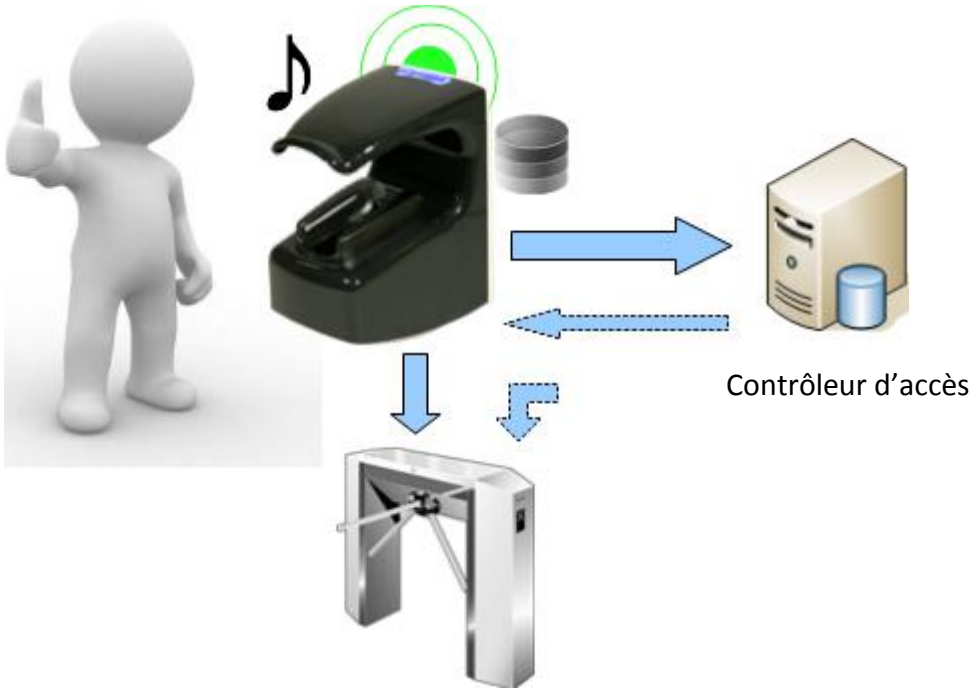
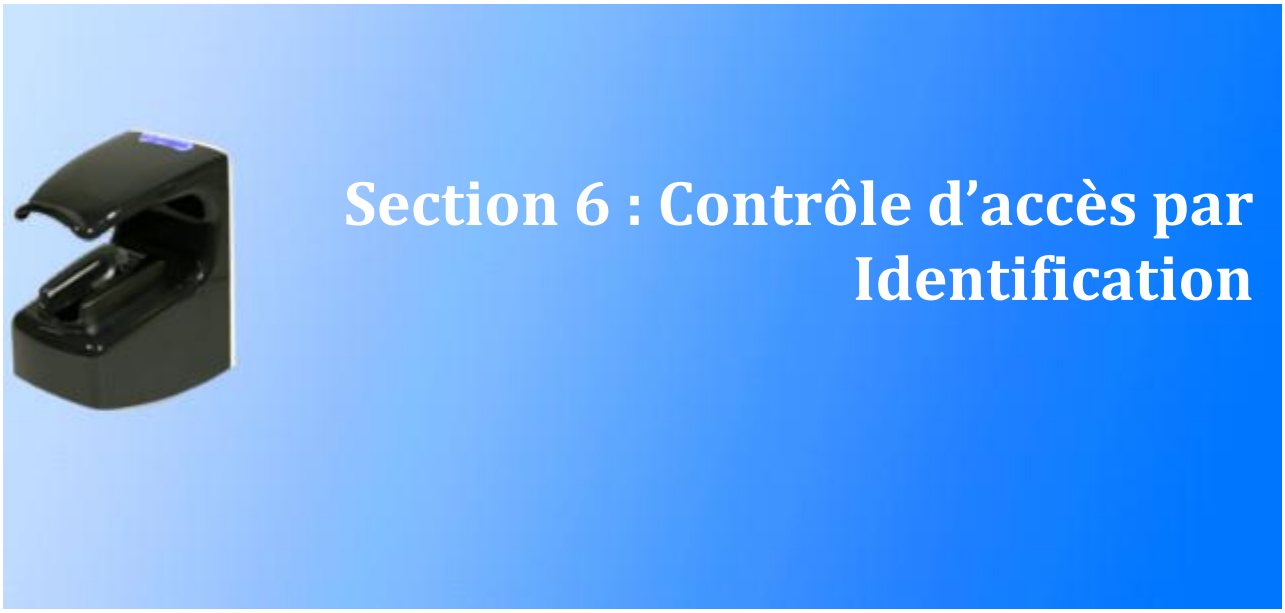


Figure 25 : Accès autorisé

Accès refusé

Figure 26 : Accès refusé



Section 6 : Contrôle d'accès par Identification

Description du mode Identification

Processus d'identification

Le processus d'identification consiste à trouver l'identité d'une personne inconnue, en comparant une donnée personnelle avec une base contenant le même type de donnée pour des personnes connues. A la fin du processus, la personne est soit identifiée (identité connue), soit toujours inconnue.

Identification appliquée au contrôle d'accès

Le processus d'identification du terminal MorphoAccess® fonctionne par comparaison des données biométriques du doigt posé sur le capteur, avec les données biométriques de tous les doigts enregistrés dans la base interne.

Cela signifie que les données biométriques des personnes dont l'accès est autorisé doivent être enregistrées dans la base du terminal avant que celle-ci demande l'accès au terminal. Ces données biométriques sont acquises soit directement sur le terminal (à l'aide de l'utilitaire MorphoEnroll), soit sur un système d'enrôlement qui utilise un capteur biométrique de même nature.

Le processus de contrôle de droits d'accès par identification est déclenché par la pose d'un doigt sur le capteur biométrique.

Lors de cette demande d'accès, l'utilisateur est inconnu, et le terminal recherche son identité. Si elle est trouvée, l'accès est autorisé, par contre s'il reste inconnu, l'accès est refusé.

Résultat du contrôle d'accès

Le résultat du contrôle d'accès est indiqué à l'utilisateur par un signal visuel et sonore émis par le terminal lui-même. Ces signaux sont décrits dans la section Résultat de la demande d'accès.

Données personnelles requises dans la base interne

Ce mode nécessite que tous les utilisateurs autorisés soient enregistrés dans la base interne du terminal. Cela signifie qu'il doit y avoir un enregistrement par utilisateur, avec chacun un identifiant unique et les données biométriques de deux des doigts de l'utilisateur.

La gestion de la base interne est décrite dans la section Gestion de la base du terminal MorphoAccess®.

Compatibilité avec un système de contrôle d'accès global

Quand le mode Identification est activé, le terminal MorphoAccess® offre les fonctions optionnelles suivantes :

- Activation du relais interne sur accès autorisé, comme décrit dans la section Activation du relais interne
- Activation externe du relais interne, comme décrit dans la section Activation externe du relais
- Envoi d'un message de résultat du contrôle local, à un système distant, comme décrit dans la section Envoi du message résultat de contrôle d'accès.
- Attente de la réponse du système distant avant d'autoriser l'accès, comme décrit dans la section Fonctionnalité LED IN

Clé d'activation

L'activation du mode identification est conditionnée à une seule clé de configuration.

Activation du mode identification	
app/bio ctrl/identification =1	Activé
app/bio ctrl/identification = 0	Désactivé

Interface utilisateur

Dans ce mode, le terminal MorphoAccess® est en attente de la présence d'un doigt sur le capteur. Cet état est signalé à l'utilisateur par un signal spécifique comme indiqué dans la section Interface lumineuse et sonore.

Pour demander l'accès, l'utilisateur pose un doigt sur le capteur biométrique, ce qui déclenche le processus d'identification.

Figure 27 : Mode Identification

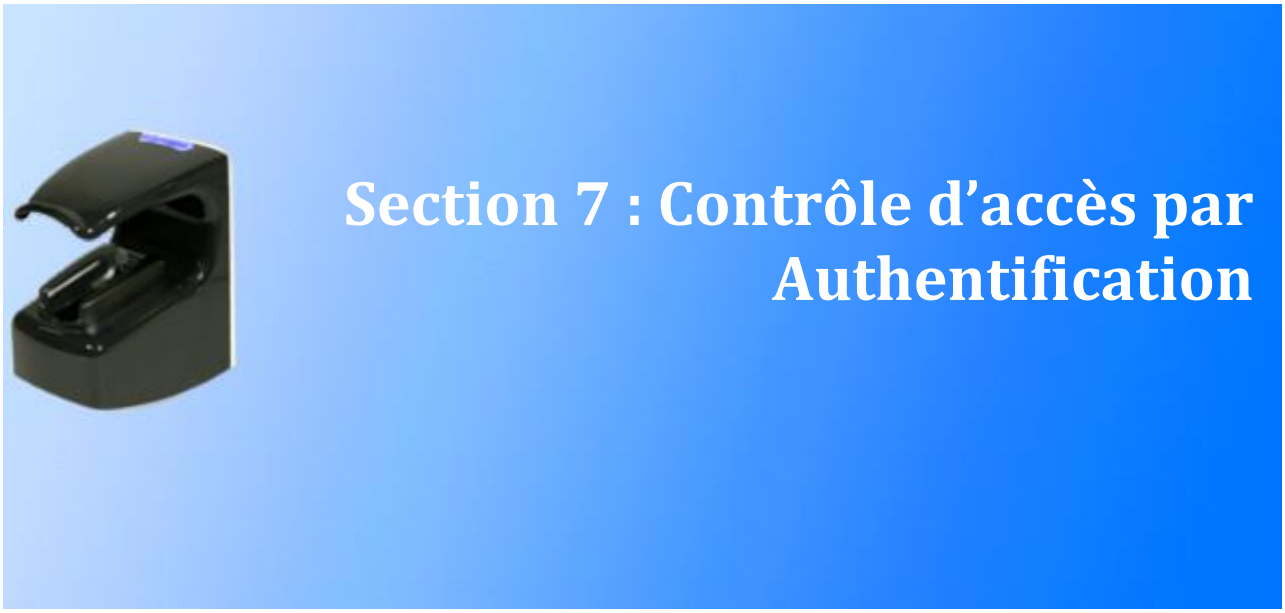
Les données biométriques du doigt posé sont capturées, puis comparées avec toutes les données biométriques enregistrées dans la base.

- Si une correspondance est trouvée, alors l'utilisateur est identifié (le terminal dispose de son identifiant), et l'accès est autorisé.
- Si aucune correspondance n'est trouvée, alors l'utilisateur reste inconnu (pas d'identifiant utilisateur), et l'accès est refusé.

Le résultat de l'identification est communiqué à l'utilisateur par un signal spécifique, comme indiqué dans la section Interface lumineuse et sonore.

A la fin du processus d'identification, quel que soit le résultat (utilisateur identifié ou toujours inconnu), le terminal se remet automatiquement en attente de pose de doigt sur le capteur.

S'il n'y a pas d'utilisateur enregistré dans la base, le processus d'identification est indisponible. Aucun utilisateur ne pourra obtenir l'accès. Cet état est indiqué à l'utilisateur, comme spécifié dans la section Interface lumineuse et sonore.


Section 7 : Contrôle d'accès par Authentification

Principes de l'authentification

Introduction

Le terminal MorphoAccess® VP propose un mode authentification conçu pour fonctionner avec des cartes à puce sans contact, utilisées comme cartes personnelles.

Cette section se rapporte donc uniquement aux terminaux équipés d'un lecteur de cartes à puce sans contact (voir section Champ d'application du document).

Dans l'ensemble du document le terme « carte » est utilisé à la place de « carte à puce sans contact ».

Processus d'authentification

Contrairement au mode « identification », l'identité de l'utilisateur doit être connue pour que le processus d'authentification puisse être exécuté.

En effet, l'authentification est un processus de vérification d'identité : l'utilisateur décline sont identité, et le terminal la vérifie en utilisant les contrôles requis.

Ce mode ne compare pas les données de l'utilisateur à celles d'autres utilisateurs : il compare les données fournies par l'utilisateur avec celle fournies pendant la phase d'enrôlement.

Authentification appliqué au contrôle d'accès

Pour décliner son identité, l'utilisateur présente sa carte d'identification personnelle qui contient son identifiant. Cette action déclenche le processus d'authentification.

Figure 28 : L'utilisateur déclenche l'authentification par présentation de sa carte

La carte de l'utilisateur contient impérativement l'identifiant de l'utilisateur, mais peut contenir aussi des données biométriques.

Le terminal effectue les vérifications d'identité prévues en utilisant les données lues sur la carte, et éventuellement des données enregistrées dans sa base interne.

Lorsqu'il a lieu, le contrôle biométrique consiste à comparer les données biométriques du doigt posé sur le capteur avec les données biométriques de deux des

doigts de l'utilisateur utilisées comme référence. Ces données de référence sont acquises lors de l'enrôlement de l'utilisateur.

Si une correspondance est trouvée le contrôle biométrique est positif : l'identité de l'utilisateur est confirmée. Sinon, en l'absence de correspondance le contrôle biométrique est négatif : l'identité de l'utilisateur n'est pas confirmée.

L'accès est autorisé uniquement lorsque l'utilisateur est authentifié (identité vérifiée).

Le terminal MorphoAccess® autorise l'activation simultanée du mode Identification et d'un mode authentification, comme indiqué dans la section Section 8 : Mode Multi-facteurs.

Carte à puce sans contact

Le terminal ignore les cartes qui sont encodées avec des clés d'authentification « carte-terminal » inconnues. Seules les demandes d'accès faites avec des cartes encodées avec les mêmes clés d'authentification « carte-terminal » que celle du terminal, seront prisent en comptes.

Le terminal refuse les cartes utilisateurs qui ne contiennent pas les données indispensables au processus d'authentification sélectionné.

Tous les modes d'authentification nécessitent la présence de l'identifiant de l'utilisateur. Les autres données et leur format dépend du processus d'authentification sélectionné.

Les données non obligatoires trouvées sur la carte sont ignorées.

Les données et leur format sur la carte de l'utilisateur, sont décrits dans le document MorphoAccess® Contactless Card Specifications.

Variantes du processus d'Authentification

Le terminal MorphoAccess® propose plusieurs processus d'authentification, suivant l'emplacement des données biométriques de l'utilisateur, et le niveau de contrôle requis.

Les données biométriques de référence de l'utilisateur sont :

- soit uniquement enregistrées sur sa carte personnelle, comme décrit dans la section Contrôle biométrique et données biométriques sur carte utilisateur
- soit enregistrées dans la base locale du terminal, comme décrit dans la section Contrôle biométrique, et données biométriques dans la base du terminal

De plus, le contrôle biométrique peut être omis comme indiqué dans les sections suivantes :

- Désactivation manuelle du contrôle biométrique
- Désactivation automatique du contrôle biométrique

Désactivation manuelle du contrôle biométrique

Par défaut, le contrôle biométrique est obligatoire, mais il peut être désactivé par l'administrateur du terminal. Dans ce cas :

- le terminal ne demande pas à l'utilisateur de poser un doigt sur le capteur.
- l'accès est autorisé sans contrôle biométrique.

Suivant le processus d'authentification choisi :

- Le terminal ne fait aucune vérification sur la valeur de l'identifiant de l'utilisateur, comme indiqué dans la section Pas de contrôle biométrique, pas de contrôle sur l'identifiant de l'utilisateur
- Le terminal vérifie la présence de l'identifiant de l'utilisateur dans la base du terminal, comme indiqué dans la section Pas de contrôle biométrique, identifiant de l'utilisateur dans la base

Désactivation automatique du contrôle biométrique

Le terminal MorphoAccess® propose un mode d'authentification qui dépend du contenu de la carte de l'utilisateur.

Sur la carte de l'utilisateur, le terminal cherche une donnée qui lui indique si le contrôle biométrique est obligatoire ou inhibé.

Ce mode d'authentification est décrit dans la section Processus d'authentification défini par la carte.

Résultat du contrôle d'accès

Le résultat du contrôle d'accès est indiqué à l'utilisateur par un signal visuel et sonore émis par le terminal lui-même. Ces signaux sont décrits dans la section Section 12 : Interface sonore et lumineuse.

Compatibilité avec un système de contrôle d'accès global

Quand le mode authentification est activé, le terminal MorphoAccess® offre les fonctions optionnelles suivantes :

- Activation du relais interne sur accès autorisé, comme décrit dans la section Activation du relais interne
- Activation externe du relais interne, comme décrit dans la section Activation externe du relais
- Envoi d'un message de résultat du contrôle local, à un système distant, comme décrit dans la section Envoi du message résultat de contrôle d'accès.
- Attente de la réponse du système distant avant d'autoriser l'accès, comme décrit dans la section Fonctionnalité LED IN

Choix du type de carte utilisateur : MIFARE® et/ou DESFire®

Type de carte sans contact

Les terminaux MorphoAccess® VP-Dual étant équipés d'un lecteur de carte sans contact compatible MIFARE® et DESFire®, il est possible de spécifier le type de carte que ce terminal peut lire :

- Soit uniquement des cartes MIFARE®
- Soit uniquement des cartes DESFire® chiffrement 3DES
- Soit uniquement des cartes DESFire® chiffrement AES
- Soit des cartes MIFARE® et des cartes DESFire® 3DES
- Soit des cartes MIFARE® et des cartes DESFire® AES
- Soit des cartes MIFARE® et des cartes DESFire® 3DES et des cartes DESFire® AES

  Les terminaux MorphoAccess® VP-Dual sont capable de lire indifféremment des cartes DESFire® ou DESFire® EV1.

  Le chiffrement AES n'est supporté que par les cartes DESFire® EV1.

  Le chiffrement 3DES utilisé pour la communication avec les cartes DESFire® EV1 est le même que celui utilisé pour les cartes DESFire® (i.e. il s'agit du mode de compatibilité des cartes DESFire® EV1).

Clé de configuration

Le choix du type de carte supporté par l'application de contrôle d'accès se fait avec la clé de configuration spécifique suivante :

Type de carte sans contact acceptées	
app/contactless/enabled profiles = 0	Carte MIFARE® uniquement (User ID au format binaire ou TLV)
app/contactless/enabled profiles = 1	Carte DESFire® 3DES uniquement (données au format TLV uniquement)
app/contactless/enabled profiles = 2	Cartes MIFARE® uniquement (données au format TLV uniquement)
app/contactless/enabled profiles = 3	Cartes MIFARE® et DESFire® 3DES (données au format TLV uniquement)
app/contactless/enabled profiles = 8	Cartes DESFire® AES uniquement (données au format TLV uniquement)
app/contactless/enabled profiles = 9	Cartes DESFire® AES et 3DES (données au format TLV uniquement)
app/contactless/enabled profiles = 10	Cartes MIFARE® et DESFire® AES (données au format TLV uniquement)

app/contactless/enabled profiles = 11	Cartes MIFARE® et DESFire® AES et 3DES (données au format TLV uniquement)

Compatibilité avec les modes « authentification »

L'utilisation d'un identifiant binaire n'est possible qu'avec des cartes MIFARE®, et lorsque la valeur de la clé de configuration « *app/contactless/enabled profiles* » est égale à 0 (zéro).

Les autres valeurs de cette clé de configuration imposent l'emploi de données enregistrées au format TLV, comme indiqué dans le document MorphoAccess® Contactless Card Specifications.

Contrôle biométrique et données biométriques sur carte utilisateur

Description

Dans ce mode, la carte de chaque utilisateur contient son identifiant personnel et les données biométriques de deux de ses doigts. Le terminal compare les données biométriques du doigt placé sur le capteur, avec celles des deux doigts de référence lues sur la carte de l'utilisateur. L'accès est autorisé, si une correspondance est trouvée, sinon l'accès est refusé.

Ce mode d'authentification n'utilise pas la base interne du terminal.

Si nécessaire, le contrôle biométrique peut être désactivé. Cette possibilité est décrite dans la section Pas de contrôle biométrique, pas de contrôle sur l'identifiant de l'utilisateur.

Données personnelles requises dans le terminal

Ce mode d'authentification n'utilise pas la base interne du terminal MorphoAccess®. Aucune donnée personnelle n'est enregistrée dans le terminal.

Données personnelles requises sur la carte de l'utilisateur

Pour être compatible avec ce mode d'authentification, la carte de l'utilisateur doit impérativement contenir :

- l'identifiant de l'utilisateur (User ID)
- les données biométriques de deux doigts de référence de l'utilisateur.

Toutes les autres données sont ignorées.

Les données enregistrées sur la carte doivent impérativement respecter le format TLV.

Le format des données sur la carte est décrit dans le document *MorphoAccess® Contactless Card Specifications*.

Clé d'Activation

Ce mode est activé par une seule clé de configuration.

Mode Authentification avec contrôle biométrique, données biométriques enregistrées sur la carte de l'utilisateur.	
app/bio ctrl/authent PK contactless = 1	Activé
app/bio ctrl/authent PK contactless = 0	Désactivé

Interface utilisateur

Le processus d'authentification commence lorsque l'utilisateur présente sa carte au-dessus du terminal (à l'endroit où se situe le lecteur de cartes sans contact). Si elle est compatible (clés d'authentification et données indispensables présentes sur la carte), le terminal invite l'utilisateur à poser son doigt sur le capteur pour le contrôle biométrique.

Figure 29 : Mode authentification avec données biométriques sur la carte

Le terminal compare alors les données biométriques du doigt sur le capteur avec les données biométriques de référence lues dans la carte de l'utilisateur.

L'authentification est positive (identité confirmée) si une correspondance est trouvées avec l'un des doigts de référence. Sinon, en l'absence de correspondance, l'authentification est négative (identité non confirmée).

Le résultat de la comparaison est signalé à l'utilisateur, par un signal sonore et lumineux, comme indiqué dans la section Résultat du contrôle d'accès.

Une fois le processus d'authentification terminé (quel que soit le résultat), le terminal retourne automatiquement en attente de la présentation d'une carte utilisateur.

Contrôle biométrique, et données biométriques dans la base du terminal

Description

Dans ce mode, seul l'identifiant de l'utilisateur (User ID) est lu sur la carte personnelle de l'utilisateur. Les données biométriques de deux des doigts de l'utilisateur sont enregistrés dans la base sous le même identifiant que celui de la carte.

Le terminal compare les données biométriques du doigt placé sur le capteur avec les données biométriques trouvées dans la base. Si une correspondance est trouvée, l'accès est autorisé, sinon (pas de correspondance), l'accès est refusé.

Données personnelles requises dans le terminal

Ce mode nécessite l'utilisation de la base interne du terminal, et la présence d'un enregistrement pour chaque utilisateur autorisé. Chaque enregistrement contient :

- le même identifiant que celui de la carte personnelle de l'utilisateur.
- les données biométriques de deux des doigts de l'utilisateur.

Si le terminal ne trouve aucun enregistrement avec le même identifiant que celui lu dans la carte, alors l'accès est refusé.

La taille et la gestion de la base interne est décrite dans la section Gestion de la base du terminal MorphoAccess®.

Données personnelles requises sur la carte

Seul l'identifiant de l'utilisateur est requis sur la carte. Les autres données sont ignorées.

Le terminal peut lire l'identifiant de l'utilisateur dans une structure TLV, ou bien directement lu à un endroit donné de la carte (identifiant binaire) (MIFARE® uniquement).

Le format TLV est décrit dans le document MorphoAccess® Contactless Card Specifications.

Clé d'activation

L'activation de ce mode est contrôlée par une seule clé de configuration.

Authentification avec données biométriques dans la base interne	
app/bio ctrl/authent ID contactless = 0	Désactivé
app/bio ctrl/authent ID contactless = 1	Activé

Interface utilisateur

Le processus d'authentification commence lorsque l'utilisateur présente sa carte au-dessus du terminal (à l'endroit où se situe le lecteur de cartes sans contact). Si l'identifiant utilisateur lu sur la carte est trouvé dans la base interne du terminal, alors le terminal demande à l'utilisateur de placer un doigt sur le capteur, pour effectuer le contrôle biométrique.

Figure 30 : Mode authentification avec données biométriques dans la base

Le terminal compare alors les données biométriques du doigt sur le capteur avec les données biométriques de référence trouvées dans la base.

L'authentification est positive (identité confirmée) si une correspondance est trouvée avec l'un des doigts de référence. Sinon, en l'absence de correspondance, l'authentification est négative (identité non confirmée).

Le résultat de la comparaison est signalé à l'utilisateur, par un signal sonore et lumineux, comme indiqué dans la section Résultat du contrôle d'accès.

Une fois le processus d'authentification terminé (quel que soit le résultat), le terminal retourne automatiquement en attente de la présentation d'une carte utilisateur.

S'il n'y a pas d'utilisateur enregistré dans la base, ce processus d'authentification est indisponible. Aucun utilisateur ne pourra obtenir l'accès par ce moyen. Cet état est indiqué à l'utilisateur, comme spécifié dans la section Etat du terminal.

Pas de contrôle biométrique, pas de contrôle sur l'identifiant de l'utilisateur

Description

Ce mode d'authentification est la version du mode « Contrôle biométrique et données biométriques sur carte utilisateur » lorsque le contrôle biométrique est désactivé.

Seul l'identifiant de l'utilisateur (User ID) est lu sur la carte personnelle de l'utilisateur. Aucun autre contrôle n'est effectué : pas de recherche de l'identifiant utilisateur dans la base, pas de contrôle biométriques.

Le terminal MorphoAccess® fonctionne comme un simple lecteur de carte sans contact.

L'accès est autorisé, simplement si la carte est encodée avec les mêmes clés que le terminal, et que le terminal peut y lire un identifiant utilisateur. Dans le cas contraire la carte est ignorée, donc l'accès est refusé.

Données personnelles requises dans le terminal

Ce mode d'authentification n'utilise pas la base du terminal. Aucune donnée personnelle n'est requise.

Données personnelles requises sur la carte de l'utilisateur

Pour être compatible avec ce mode d'authentification, la carte de l'utilisateur doit contenir un identifiant utilisateur (User ID). Celui-ci peut être enregistré au format TLV, ou être une donnée binaire à lire sur la carte (MIFARE® uniquement).

Toutes les autres données sont ignorées.

Le format TLV est décrit dans le document *MorphoAccess® Contactless Card Specifications*.

Le terminal MorphoAccess® n'effectue aucun contrôle sur la valeur de l'identifiant de l'utilisateur.

Clé d'activation

Ce mode d'authentification est activé par deux clés de configuration.

Authentification sans contrôle biométrique et sans contrôle sur l'identifiant de l'utilisateur.	
app/bio ctrl/authent PK contactless = 1	Enabled
app/bio ctrl/bypass authentication = 1	Enabled

Interface Utilisateur

Le processus d'authentification commence lorsque l'utilisateur présente sa carte au-dessus du terminal (à l'endroit où se situe le lecteur de cartes sans contact).

Figure 31: Authentification sans contrôle biométrique, et sur l'identifiant utilisateur

Si l'identifiant de l'utilisateur peut être lu sur la carte, l'accès est autorisé, sinon l'accès est refusé.

Le résultat de la comparaison est signalé à l'utilisateur, par un signal sonore et lumineux, comme indiqué dans la section Résultat du contrôle d'accès.

Une fois le processus d'authentification terminé (quel que soit le résultat), le terminal retourne automatiquement en attente de la présentation d'une carte utilisateur.

Pas de contrôle biométrique, identifiant de l'utilisateur dans la base

Description

Ce mode d'authentification est la version du mode « Contrôle biométrique, et données biométriques dans la base du terminal » lorsque le contrôle biométrique est désactivé.

Seul l'identifiant de l'utilisateur (User ID) est lu sur la carte personnelle de l'utilisateur. Le terminal le recherche dans la base, mais n'effectue pas de contrôle biométriques.

L'accès est autorisé si l'identifiant de l'utilisateur, lu sur la carte, est trouvé dans la base. Dans le cas contraire, l'accès est refusé.

Données personnelles requises dans le terminal

Ce mode nécessite l'utilisation de la base interne du terminal, et la présence d'un enregistrement pour chaque utilisateur autorisé. Chaque enregistrement contient :

- le même identifiant que celui de la carte personnelle de l'utilisateur.
- les données biométriques de deux des doigts de l'utilisateur.

Si le terminal ne trouve aucun enregistrement avec le même identifiant que celui lu dans la carte, alors l'accès est refusé.

La taille et la gestion de la base interne est décrite dans la section Gestion de la base du terminal MorphoAccess®.

Données personnelles requises sur la carte de l'utilisateur

Pour être compatible avec ce mode d'authentification, la carte de l'utilisateur doit contenir un identifiant utilisateur (User ID). Celui-ci peut être enregistré au format TLV, ou être une donnée binaire à lire sur la carte. (MIFARE® uniquement). Toutes les autres données sont ignorées.

Le format TLV est décrit dans le document *MorphoAccess® Contactless Card Specifications*.

Clé d'activation

Ce mode d'authentification est activé par deux clés de configuration.

Authentification sans contrôle biométrique, mais l'identifiant de l'utilisateur doit être dans la base	
app/bio ctrl/authent ID contactless = 1	Enabled
app/bio ctrl/bypass authentication = 1	Enabled

Interface utilisateur

Le processus d'authentification commence lorsque l'utilisateur présente sa carte au-dessus du terminal (à l'endroit où se situe le lecteur de cartes sans contact).

Figure 32: Authentification sans contrôle biométrique, et sur l'identifiant utilisateur

L'identifiant de l'utilisateur lu sur la carte est recherché dans la base.

Le processus d'authentification est positif (identité confirmée) si l'identifiant utilisateur lu sur la carte est trouvé dans la base du terminal, sinon il est négatif (identité non confirmée).

Le résultat de la comparaison est signalé à l'utilisateur, par un signal sonore et lumineux, comme indiqué dans la section Résultat de la demande d'accès.

Une fois le processus d'authentification terminé (quel que soit le résultat), le terminal retourne automatiquement en attente de la présentation d'une carte utilisateur.

Processus d'authentification défini par la carte

Description

Lorsque ce mode est activé, un champ spécifique de la carte de l'utilisateur spécifie le type de contrôle à effectuer. Ainsi, le même terminal peut exécuter un processus différent suivant la carte présentée :

- Soit le contrôle biométrique est effectué avec les données biométriques de référence trouvées sur la carte de l'utilisateur
- Soit le contrôle biométrique est inhibé et seule la présence de l'identifiant de l'utilisateur est vérifiée.

Une carte qui inhibe le contrôle biométrique est utile dans le cas où la capture des données biométriques n'est pas nécessaire (par exemple pour un « visiteur » de courte durée) ou impossible (physiquement ou légalement). Ces cartes peuvent être réalisées à l'avance et être utilisées pour différents visiteurs.

La base interne du terminal n'est pas utilisée.

Données personnelles requises dans la base du terminal

Ce mode d'authentification n'utilise pas la base interne du terminal MorphoAccess®. Aucune donnée personnelle n'est enregistrée dans le terminal.

Données requises sur carte de l'utilisateur

Pour être compatible avec ce mode d'authentification, la carte doit contenir les données suivantes : l'identifiant de l'utilisateur et l'indicateur de processus.

Si le contrôle biométrique est obligatoire, la carte doit impérativement contenir les données biométriques de deux des doigts de l'utilisateur.

Toute autre donnée présente est ignorée.

Toutes ces données doivent être enregistrées au format TLV.

Le format des données sur la carte est décrit dans le document *MorphoAccess® Contactless Card Specifications*.

Clé d'activation

Ce mode est activé par une seule clé de configuration.

Mode authentification défini par la carte de l'utilisateur	
app/bio ctrl/authent card mode =1	Désactivé
app/bio ctrl/authent card mode = 0	Activé

Interface utilisateur

Démarrage

Le processus d'authentification commence lorsque l'utilisateur présente sa carte au-dessus du terminal (à l'endroit où se situe le lecteur de cartes sans contact).

Le terminal cherche sur la carte de l'utilisateur la donnée qui lui indique si le contrôle biométrique est obligatoire ou désactivé. Si elle est présente, le terminal exécute ou pas le contrôle biométrique, suivant le contenu de cette donnée :

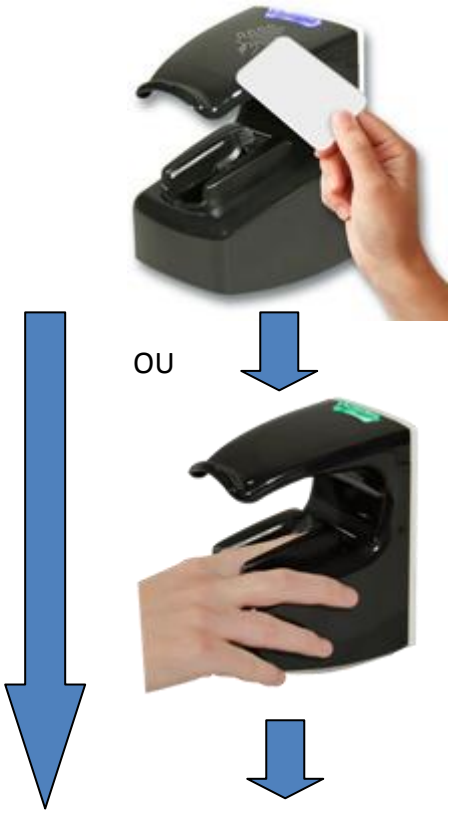


Figure 33 : Processus d'authentification défini par la carte

Le résultat de la comparaison est signalé à l'utilisateur, par un signal sonore et lumineux, comme indiqué dans la section Résultat du contrôle d'accès.

Une fois le processus d'authentification terminé (quel que soit le résultat), le terminal retourne automatiquement en attente de la présentation d'une carte utilisateur.

Contrôle biométrique obligatoire

Le terminal demande à l'utilisateur de poser un doigt sur le capteur. Puis il effectue une comparaison biométrique entre le doigt présenté sur le capteur et les données biométriques de référence lues sur la carte de l'utilisateur.

Le processus exécuté est identique à celui décrit dans la section Contrôle biométrique et données biométriques sur carte utilisateur.

Contrôle biométrique inhibé

Le résultat de la vérification est immédiat, avec seulement l'identifiant utilisateur.

Le terminal ne demande pas à l'utilisateur de poser le doigt sur le capteur biométrique, et n'effectue aucune comparaison biométrique.

Le processus exécuté est identique à celui décrit dans la section Pas de contrôle biométrique, pas de contrôle sur l'identifiant de l'utilisateur.

Formats supportés pour l'identifiant utilisateur

Format TLV

L'identifiant de l'utilisateur est enregistré en ASCII dans une structure TLV.

L'identifiant de l'utilisateur est écrit au format TLV	
app/contactless/data format = 0	Structure TLV
app/contactless/data length= 0.0	Détection automatique de taille
app/contactless/data offset= 0.0	Détection automatique du début

Le format des données enregistrées sur la carte sans contact de l'utilisateur est décrit dans le document : *MorphoAccess® Contactless Card Specifications*.

ISO14443 type A UID

Description

Le terminal MorphoAccess® est capable d'utiliser le Card UID type A de la norme ISO 14443, comme identifiant utilisateur.

Le Card UID est une caractéristique propre à chaque carte MIFARE® et à chaque carte DESFire®.

Le Card UID peut être acquis dans les deux sens (Most Significant Byte ou Less Significant Byte.

Compatibilité avec le type de carte

Ce format ne peut être utilisé que lorsque le mode est « Carte MIFARE® uniquement (identifiant de l'utilisateur au format binaire ou TLV) ».

Type de carte sans contact autorisé	
app/contactless/enabled profiles = 0	Lorsque la clé est à 0, le terminal est capable de lire le Card UID des cartes MIFARE® et des cartes DESFire®.

Clés de configuration

app/ bio ctrl/AC_ID	
CARDDATA	Structure TLV: doit être retiré
CARDSN:STD	ISO14443 type A UID, sens MSB. Un Card UID égal à 0xFEA7B152 produit un identifiant égal à 4272402770
CARDSN:REV	ISO14443 type A UID, sens LSB. Un Card UID égal à 0xFEA7B152 produit un identifiant égal à 1387374590.

Une autre clé de configuration spécifie quel type d'identifiant déclenche le processus de contrôle d'accès.

Donnée utilisée pour commencer le contrôle d'accès	
app/contactless/ event on = 1	ISO 14443 type A Card UID (Unique IDentifier)

Valeur binaire

Description

Le terminal MorphoAccess® peut utiliser comme identifiant utilisateur, une valeur binaire, lue sur la carte à un endroit précis.

Il est possible d'utiliser le numéro de série de la carte, comme indiqué dans le paragraphe Exemple - numéro de série de carte MIFARE® (format Big Endian).

Le terminal MorphoAccess® peut lire une valeur binaire non cadrée sur des octets entiers. Ceci est utile pour lire un identifiant utilisateur inclus dans une trame Wiegand enregistrée sur la carte de l'utilisateur. Ce cas est décrit dans le paragraphe Exemple : Identifiant de 32 bits dans une trame Wiegand.

Aucune structure TLV n'est requise dans la carte, ainsi le terminal MorphoAccess® peut s'adapter à des cartes encodées par d'autres systèmes.

Compatibilité avec les types de carte

Ce format ne peut être utilisé qu'avec le mode par défaut «cartes MIFARE® uniquement ».

Sélection du type de carte	
app/contactless/enabled profiles = 0	Carte MIFARE® uniquement (identifiant de l'utilisateur au format binaire ou TLV).

Clés de configuration

La donnée binaire à lire est définie par :

- Le premier block contenant la donnée
- L'adresse relative du premier octet et du premier bit de la donnée, à l'intérieur du secteur. Cette valeur ne doit pas dépasser 15 octets. Le terminal est capable de lire une donnée qui ne commence pas sur un octet complet.
- La longueur en octets et en bits additionnels de la donnée, celle-ci ne doit pas dépasser 8 octets. Le terminal est capable de lire une donnée dont la longueur n'est pas un multiple de 8 bits.
- La direction de lecture : MSB or LSB

Identifiant utilisateur à lire au format binaire	
app/contactless/dataformat = 1	Format binaire
app/contactless/B	[1-215] Premier block à lire sur la carte
app/contactless/data length [nombre d'octets].[bits supplémentaires]	La taille maximale de l'identifiant utilisateur est limitée à 8 octets (soit 8.0).
app/contactless/data offset [nombre d'octets].[bits supplémentaires]	Emplacement relatif (par rapport au début du bloc) du 1er octet et du 1er bit de la donnée : 15 octets maximum (soit 15.0)
app/contactless/data type	Méthode de lecture des octets : 0.1 (données binaire, MSB first) 0.0 (données binaire, LSB first)

Exemple : numéro de série de carte MIFARE®

Dans cet exemple, le terminal est configuré pour lire les 4 premiers octets, dans le sens MSB, du 1er bloc d'une carte MIFARE®. C'est là que se trouve le numéro de série de la carte.

Si les octets lus sont F4 E1 65 34, alors l'identifiant de utilisateur est « 4108412212 » (ASCII).

Activation of identification mode	
app/contactless/data format= 1	Format binaire
app/contactless/data type= 0.1	Format binaire à lire dans le sens MSB.
app/contactless/data length = 4.0	Taille = 4 octets
app/contactless/data offset= 0.0	Premier octet du bloc
app/contactless/B= 1	Premier bloc de la carte

Exemple : Identifiant utilisateur de 32 bits dans une trame Wiegand de 37 bits

Dans cet exemple, la carte de l'utilisateur contient, dans le premier bloc du secteur n°15, une trame Wiegand de 37 bits complète (avec bit de début de trame, bit de fin de trame, et code du site émetteur). Le premier bloc du secteur n°15, est le bloc n°46.

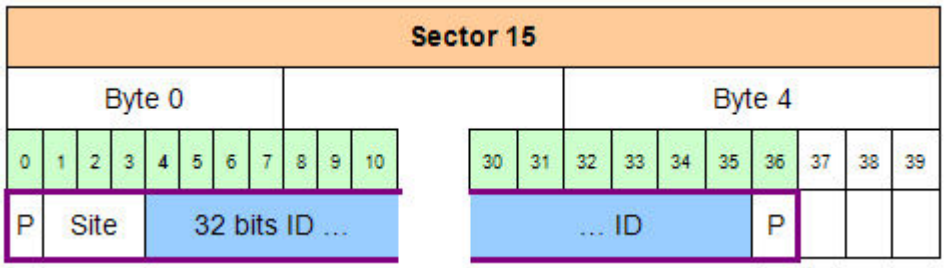
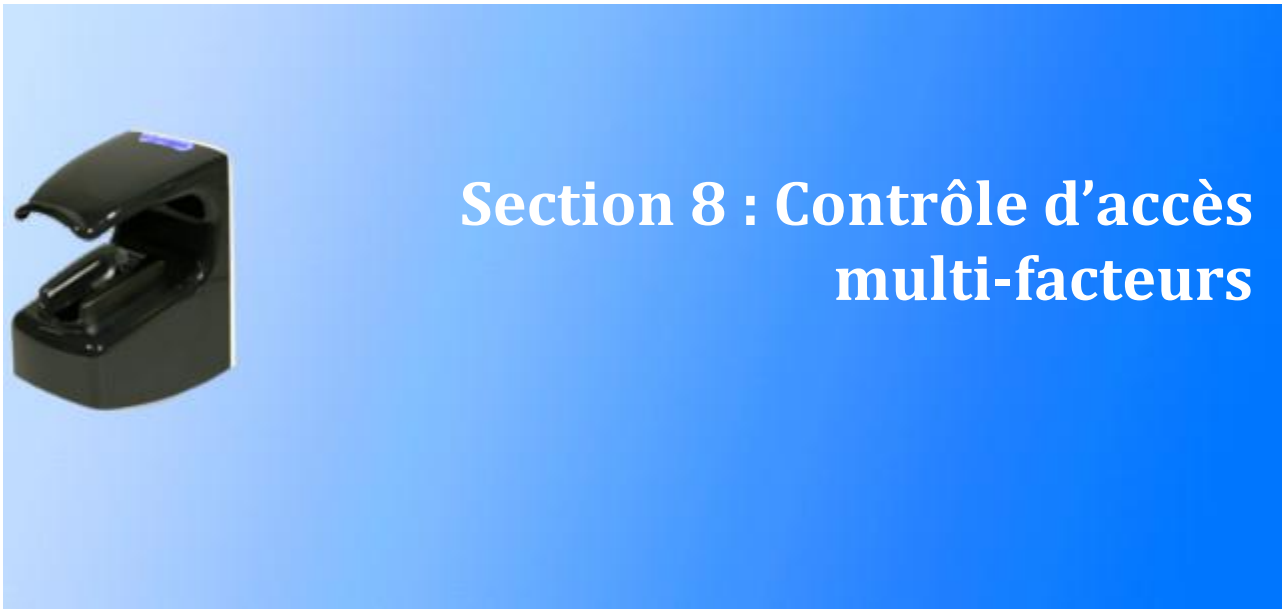


Figure 34 : Utilisation d'une trame Wiegand comme User ID

L'identifiant de 32 bits commence au bit 4. Il est précédé du bit de début de trame (bit0), et du code du site émetteur (bit1-2-3), et il est suivi du bit de fin de trame.

Acquisition identifiant utilisateur à 32 bits dans trame Wiegand de 37 bits.	
app/contactless/data format= 1	Format binaire
app/contactless/data type= 0.1	Format binaire à lire dans le sens MSB.
app/contactless/data length = 4.0	Taille = 4 octets
app/contactless/data offset = 0.4	L'identifiant utilisateur commence au bit 4 du 1er octet du bloc indiqué ci-dessous.
app/contactless/B = 15	Lecture à partir du 1er bloc du secteur n°15 (soit le bloc n°46)

Le terminal peut être configuré pour que le bit de début de trame et le code de site soit ajouté devant l'identifiant de l'utilisateur, lorsque celui-ci doit être envoyé à un système distant en utilisant le protocole Wiegand.



Section 8 : Contrôle d'accès multi-facteurs

Description du mode Multi-facteurs

Description

Le terminal MorphoAccess® autorise l'activation simultanée du mode de contrôle d'accès par identification et de l'un des modes de contrôle d'accès par authentification.

C'est la première action de l'utilisateur qui sélectionne automatiquement le processus de contrôle de droit d'accès à exécuter.

Interface utilisateur

Dans ce mode le terminal est en attente de présentation d'un doigt ou d'une carte. Il exécute :

- Le processus d'authentification si l'utilisateur présente d'abord sa carte personnelle.
- Le processus d'identification si l'utilisateur place d'abord son doigt sur le capteur

Figure 35 : Mode Multi-facteurs (identification et authentification)

En l'absence de base de données, l'utilisateur ne peut plus s'identifier (en posant son doigt), mais il lui est toujours possible de s'authentifier (en présentant sa carte).

Données personnelles requises dans la base interne

Ce sont les mêmes que celle requises par le mode « identification ».

Ce sont également celle requises lorsque le mode authentification est activé. Merci de consulter la section correspondante.

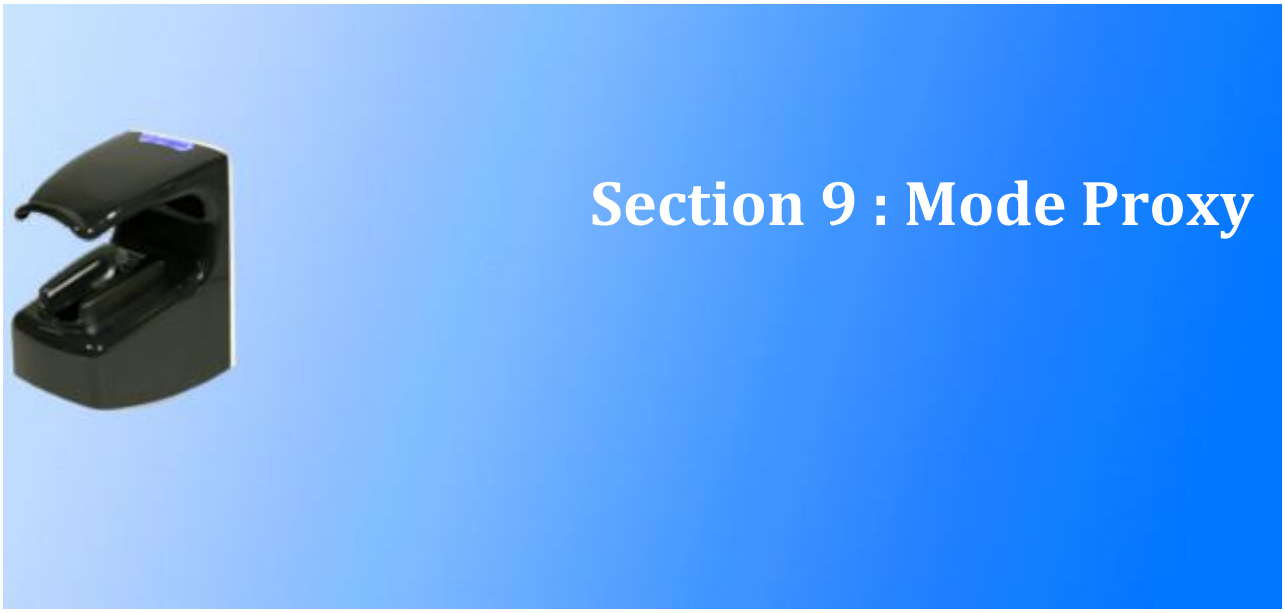
Données requises sur carte de l'utilisateur

Le ou les éléments requis dans la carte dépendent du mode d'authentification activé. Merci de consulter la section correspondante.

Clés d'activation

Ce mode est mis en service en activant le mode Identification, ainsi que l'un des modes authentification.

Mise en service du mode multi-facteur	
app/bio ctrl/identification =1	Activé
app/bio ctrl/authent card mode = 1 ou app/bio ctrl/authent ID contactless = 1 ou app/bio ctrl/authent PK contactless = 1	Activé Activé Activé


Section 9 : Mode Proxy

Présentation du mode Proxy (ou esclave)

Principe

Le mode Proxy est le mode de fonctionnement où l'application de contrôle des droits d'accès est située sur un système distant. Le terminal n'est pas autonome contrairement aux modes identification et authentification.

Cela signifie que le terminal fonctionne en esclave d'un système distant. L'application de contrôle d'accès tourne sur un système distant qui utilise les fonctions de haut niveau du terminal MorphoAccess® :

- Fonction d'identification
- Fonction d'authentification
- Fonction de lecture de données sur une carte à puce
- Fonctions de signalisation du résultat du contrôle de droit d'accès

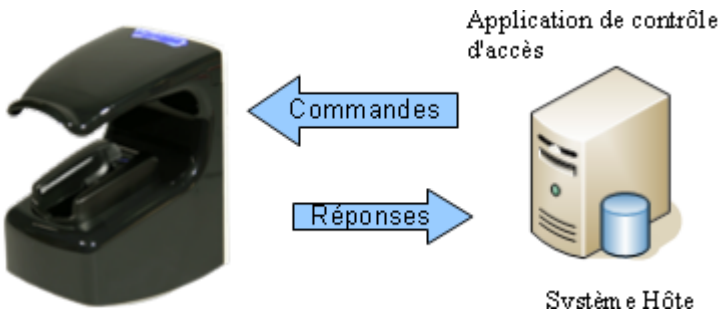


Figure 36 : Mode Proxy (esclave)

Le terminal MorphoAccess® VP est piloté, à travers une liaison Ethernet (ou Wi-Fi™) en utilisant le protocole TCP/IP ou SSL.

Le terminal fonctionne comme un serveur : soit en attente d'une commande, soit en cours d'exécution d'une commande.

Les commandes acceptées par le terminal sont décrites dans le document *MorphoAccess® Host System Interface Specifications*.

La méthode de sécurisation des données échangées, utilisant le protocole SSL, est décrite dans le document *SSL Solution for MorphoAccess®*.

Signaux locaux

Lorsque le terminal est en attente de commande de la part du système distant, il n'y a aucun signal local (retro-éclairage capteur éteint, voyant d'état éteint).

Par contre, lorsqu'une commande est en cours d'exécution, le terminal émet le signal correspondant à la fonction.

Cela signifie, par exemple, que :

- lorsque terminal exécute la commande « Identification », il émet les mêmes signaux que le mode identification autonome
- lorsque le terminal reçoit la commande « accès autorisé », il émet le signal « accès autorisé » à l'utilisateur, comme décrit dans la section Résultat du contrôle d'accès.

Les signaux sont donc tels que décrits dans la section IHM Lumineuse et sonore.

Exemple d'utilisation du mode Proxy

L'exemple ci-dessous décrit les échanges entre le terminal et le système distant dans le cadre d'un processus de contrôle de droit d'accès par identification.

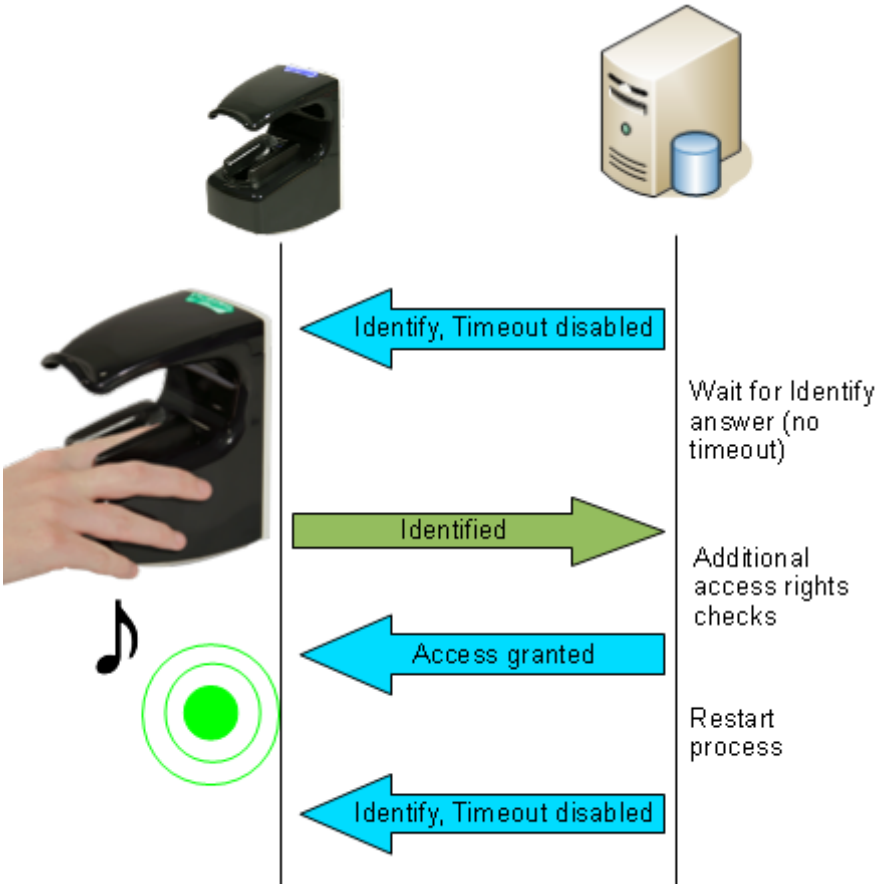
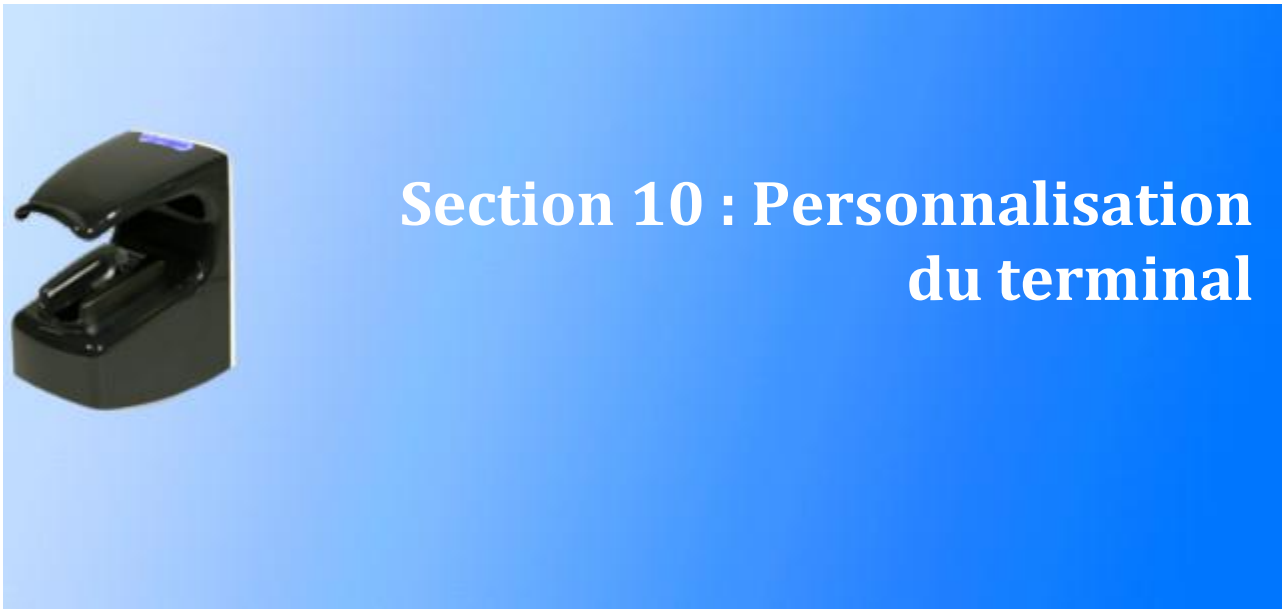


Figure 37 : Exemple d'utilisation du mode Proxy, pour un processus d'identification distant

Activation du mode Proxy

Pour activer le mode Proxy, il faut désactiver tous les modes de contrôle d'accès autonomes. C'est-à-dire que le mode identification et tous les modes authentification doivent être désactivés.

Activation du mode Proxy	
app/bio ctrl/identification = 0	Désactivé
app/bio ctrl/authent card mode = 0	Désactivé
app/bio ctrl/authent PK contactless = 0	Désactivé
app/bio ctrl/authent ID contactless = 0	Désactivé



Section 10 : Personnalisation du terminal

Nombre d'essais de comparaison biométrique

Description

Afin de réduire le taux de faux rejet (FRR), le terminal permet à l'utilisateur de poser une 2ème fois le doigt sur le capteur, dans le cas ou la comparaison biométrique initiale échoue. Ce 2ème essai est autorisé par défaut, mais il est possible de le supprimer.

Lors de ce 2ème essai, l'utilisateur peut améliorer la pose de son doigt, ou poser le bon doigt en cas d'erreur. De plus, toujours pour augmenter le taux de réussite, le terminal utilise pour le 2ème essai une méthode de reconnaissance plus poussée (mais légèrement plus lente).

Clé de configuration

Le 2ème essai peut être supprimé avec une seule clé de configuration.

Nombre maximal de comparaison biométriques	
app/bio ctrl/nb attempts = 1	Une seule comparaison autorisée (pas de 2ème essai)
app/bio ctrl/nb attempts = 2	2ème essai autorisé en cas d'échec du 1er (mode par défaut)

Mode identification

Si le doigt de l'utilisateur n'est pas reconnu, il dispose de 5 secondes pour présenter à nouveau un doigt. Au delà de ce délai, la pose d'un doigt est considérée comme une nouvelle demande d'accès.

Ce délai est réglable avec une clé de configuration.

Délai d'attente de la 2ème pose de doigt (en secondes)	
app/bio ctrl/identification timeout	5 (1-60)

Mode authentification

Si le doigt placé initialement sur le capteur n'est pas reconnu, le terminal demande à l'utilisateur de placer à nouveau un doigt, sans l'obliger à représenter sa carte.

Le délai d'attente du doigt sur le capteur est défini par une seule clé de configuration.

Délai d'attente du doigt sur le capteur en mode authentification (en secondes)	
app/bio ctrl/authent timeout	10 (1-60)

Configuration du seuil de comparaison

Description

Les performances d'un système biométrique sont mesurées principalement par deux caractéristiques :

- le taux de Faux Rejets (FRR) : nombre de personnes à qui l'accès est refusé, alors que ces personnes auraient du être autorisées à accéder, divisé par le nombre total de demandes d'accès
- le taux de Fausses Acceptations (FAR) : nombre de personnes à qui l'accès à été refusé alors qu'elles y sont autorisées, divisé par le nombre total de demandes d'accès

Le terminal MorphoAccess® autorise le réglage du FAR suivant les besoins, mais la valeur de ces deux caractéristiques sont inversement liées. C'est-à-dire que lorsque l'on règle une valeur dans un sens, l'autre valeur évolue dans l'autre sens.

Lorsque le confort de l'utilisateur est le plus important, le nombre de faux rejets doit être faible, ce qui accroit le nombre de fausse acceptations. Inversement, si la sécurité est plus importante, le nombre des fausses acceptations doit être faible, ce qui accroit le nombre de faux rejets.

Différents réglages sont proposés dans le terminal MorphoAccess® en fonction du niveau de sécurité ciblé.

Clé de configuration

Le taux de fausse acceptation est réglable par une clé de configuration : plus la valeur du paramètre est élevée plus le taux de fausse acceptation est bas.

Valeur du seuil de comparaison	
bio/bio ctrl/matching th	3 (1-10)

Les valeurs du seuil de comparaison sont détaillées dans le tableau ci-dessous.

Value	Description
0	Valeur la plus basse : le nombre de faux rejets est très bas, mais le nombre de fausse acceptations trop élevé pour une utilisation sûre. L'utilisation de cette valeur est fortement déconseillée, car le terminal devient trop permissif.
1	FAR < 1 %
2	FAR < 0.5 %
3	**FAR < 0.1%** **Valeur par défaut, recommandée pour les applications de contrôle de droit d'accès par identification.**
4	FAR < 0.05 %
5	FAR < 0.01 %
6	FAR < 0.001 %
7	FAR < 0.0001 %
8	FAR < 0.00001 %
9	FAR < 0.0000001 %
10	Valeur la plus haute : le nombre de fausse acceptations est très bas, mais le nombre de faux rejets trop élevé pour une utilisation confortable. L'utilisation de cette valeur est fortement déconseillée, car le terminal devient trop restrictif.

Niveau de sécurité Multimodal

Description

Les terminaux de la Série MorphoAccess® VP autorisent le choix du niveau de sécurité de la biométrie multimodale.

Clé de configuration

Le niveau de sécurité de la technologie multimodale est réglé par une seule clé de configuration.

Niveau de sécurité de la biométrie multimodale	
app/bio ctrl/security level = STANDARD	Niveau de sécurité standard (valeur par défaut)
app/bio ctrl/security level = MEDIUM	Niveau de sécurité intermédiaire.
app/bio ctrl/security level = HIGH	Niveau de sécurité haut.

Utiliser les niveaux de sécurité MEDIUM et HIGH pour accroître le niveau de protection contre la fraude (peut affecter le taux de faux rejets ainsi que le temps de réponse).

NB : En fonction de la configuration usine du terminal, la valeur « STANDARD » peut ne pas être disponible. Dans ce cas, la valeur par défaut est « MEDIUM ».

Détecteurs anti-intrusion et anti-arrachement

Description

Le terminal MorphoAccess® VP, est capable de détecter deux types d'événements inhabituels :

- la trappe inférieure est retirée (grâce au contrôle des détecteurs anti-intrusion)
- le terminal est retiré du mur (grâce au contrôle des détecteurs anti-arrachement)

Lorsque l'un de ces événements est détecté, le terminal agit en fonction de sa configuration :

- ignorer l'événement (par défaut) : utile lors des opérations de maintenance normales
- envoyer un message d'alarme à un système distant, par le même canal que les messages de résultat de contrôle d'accès (voir section Envoi du message résultat de contrôle d'accès).
- Emettre un signal d'alarme sonore et visuel local (voir section Etat du terminal)

Le format du message d'alarme est décrit dans le document MorphoAccess® Remote Messages Specification.

Pour plus d'informations sur l'emplacement des détecteurs anti-intrusion et anti-arrachement, merci de consulter le document Guide d'installation du MorphoAccess® VP Series

Figure 38: Interrupteurs anti-intrusion

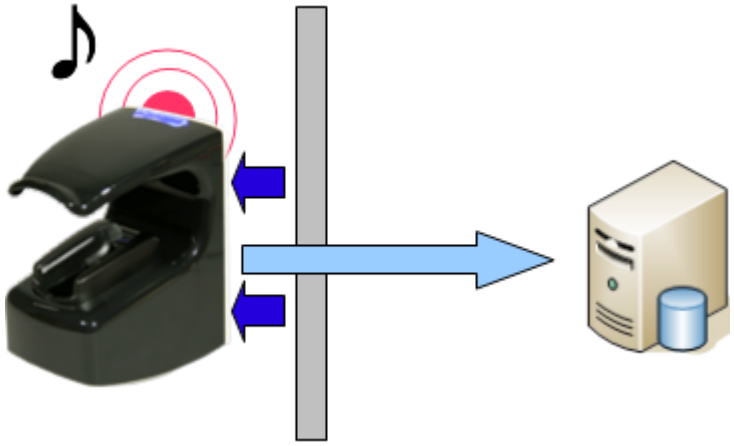


Figure 39 : Interrupteurs anti-arrachement

Clés de configuration

La (ou les) action(s) à exécuter par le terminal en cas de détection d'intrusion et/ou d'arrachement est (sont) définie(s) par une clé de configuration.

Action sur détection d'arrachement ou d'intrusion	
app/tamper alarm/level = 0	**Inhibé**: aucune action (mode par défaut)
app/tamper alarm/level = 1	**Emission d'un message**: envoi d'un message d'alarme à un système distant.
app/tamper alarm/level = 2	**Emission d'un message et alarme locale**: en plus d'émettre un message vers un système distant, le terminal émet un signal d'alarme local (sonore et visuel)

Comme le message d'alarme intrusion/arrachement est envoyé par le même port/protocole que les messages de résultat de contrôle d'accès, il faut que cette fonction soit active, sinon le message d'alarme n'est pas envoyé (voir la section Envoi du message résultat de contrôle d'accès).

De plus si le message d'alarme doit être envoyé en Wiegand ou en DataClock, il faut :

- Autoriser l'envoi de messages d'erreur en Wiegand et en DataClock
- spécifier l'identifiant du message d'alarme, si la valeur par défaut ne convient pas

Envoi du message d'alarme en Wiegand ou DataClock	
app/failure ID/alarm ID=1	Emission de message d'erreur autorisée
Envoi du message d'alarme en Wiegand ou DataClock	
app/failure ID/alarm ID	65535 (0 – 65535) Identifiant du message d'alarme « intrusion ou arrachement »

Exemple 1 : envoi message alarme en Wiegand et signal alarme local.

Dans cet exemple, en cas de détection d'intrusion ou d'arrachement, le terminal doit :

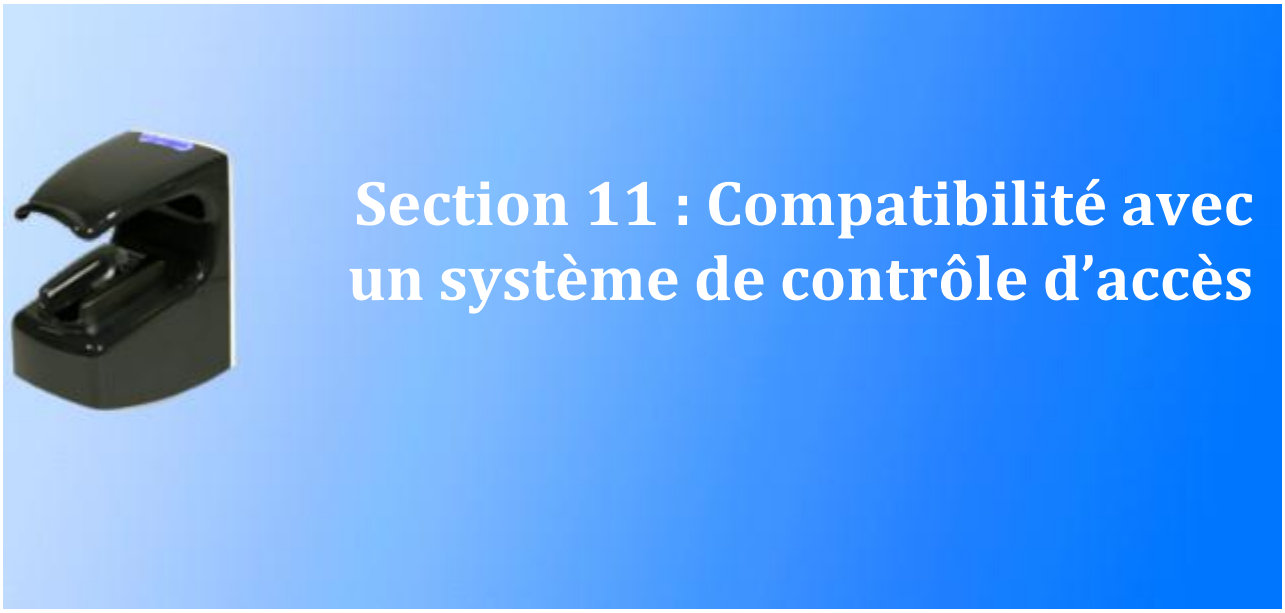
- Émettre un message d'erreur sur le port série en Wiegand. L'identifiant de cette alarme est 62221
- Emettre un signal d'alarme local sonore et lumineux

Envoi erreur 62221 en Wiegand et signal d'alarme locale	
app/tamper alarm/level=2	Intrusion ou arrachement : Envoi message d'alarme et émission signal d'alarme locale
app/failure ID/enabled=1	Envoi de message d'erreur autorisé (port série, protocole Wiegand ou DataClock)
app/failure ID/alarm ID=62221	**Inhibé**: aucune action (mode par défaut)

Exemple 2 : envoi message d'alarme en UDP

Dans cet exemple, en cas de détection d'intrusion ou d'arrachement, le terminal doit émettre un message d'erreur en UDP sur le port Ethernet (ou Wi-Fi™).

Envoi message d'alarme intrusion/arrachement en UDP	
app/tamper alarm/level=1	Intrusion ou arrachement : Envoi message d'alarme uniquement
app/send ID UDP/ enabled =1	Autorise l'envoi du message de résultat de contrôle d'accès en UDP


Section 11 : Compatibilité avec un système de contrôle d'accès

Activation du relais interne sur accès autorisé

Description

Si le contrôle est réussi, un relais peut être activé pour contrôler directement une porte.

L'installation de contrôle d'accès utilisant le relais interne offre un niveau de sécurité plus faible qu'une installation équipée d'un contrôleur d'accès central pour la gestion des autorisations d'accès. C'est la raison pour laquelle Morpho recommande l'utilisation d'un contrôleur d'accès central. Cependant, le choix de la solution à mettre en œuvre est de la responsabilité de l'installateur ou du donneur d'ordre.

Après un contrôle biométrique réussi, le relais du terminal MorphoAccess® peut être activé pendant une période spécifiée (par exemple, pour déverrouiller une porte).

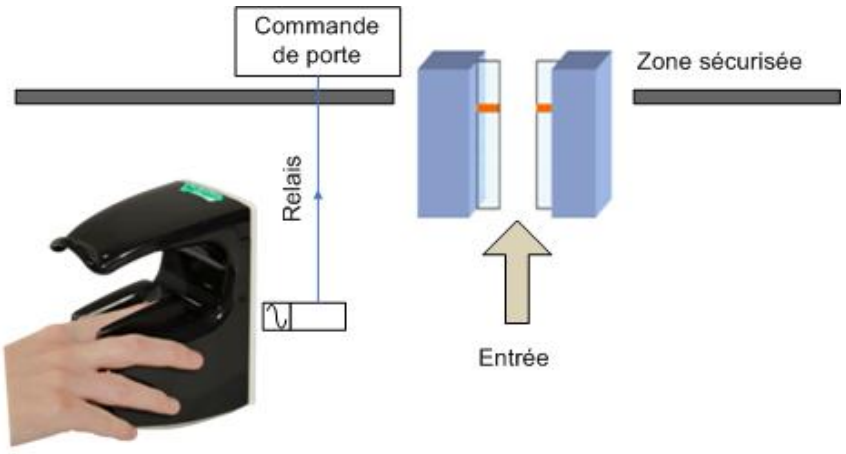


Figure 40 : Utilisation du relais interne du terminal MorphoAccess®

Clé d'activation

Une clé de configuration permet de spécifier si le relais interne doit, ou non, être activé en cas d'accès autorisé.

Activation du relais interne sur accès autorisé	
app/relay/enabled = 0	Activé (valeur par défaut)
app/relay/enabled = 1	Désactivé

Clés de configuration

Le temps d'ouverture du relais est réglable par unité de 10 ms (pour 3 secondes, la valeur doit être égale à 300).

Temps d'activation du relais (en multiple de 10 ms). Défaut : 3 secondes	
app/relay/aperture time in 10 ms	300 (50 to 60000)

Le temps d'ouverture du relai n'est pas bloquant : une demande d'accès peut être faite pendant le temps d'ouverture du relais.

L'état par défaut du relais peut également être défini.

Etat du contact du relais au repos	
app/relay/relay default state = 0	Ouvert (défaut)
app/relay/relay default state =1	Fermé

Activation externe du relais

Description

Cette fonction autorise l'activation du relais interne du terminal par un bouton-poussoir connecté entre la borne LED1 et la borne GND. Cela permet d'activer le relais dans deux cas : lorsque le terminal autorise l'accès après contrôle des droits, et lorsqu'un contact se ferme entre les bornes LED1 et GND.

Une application typique est de commander le verrouillage d'une porte par le relais du terminal MorphoAccess®, comme indiqué dans le schéma ci-dessous.

- Pour entrer dans le bâtiment, l'utilisateur doit être reconnu par le terminal MorphoAccess®.
- Pour quitter le bâtiment, l'utilisateur doit simplement appuyer sur un bouton-poussoir connecté entre les bornes LED1 et GND du terminal MorphoAccess®.

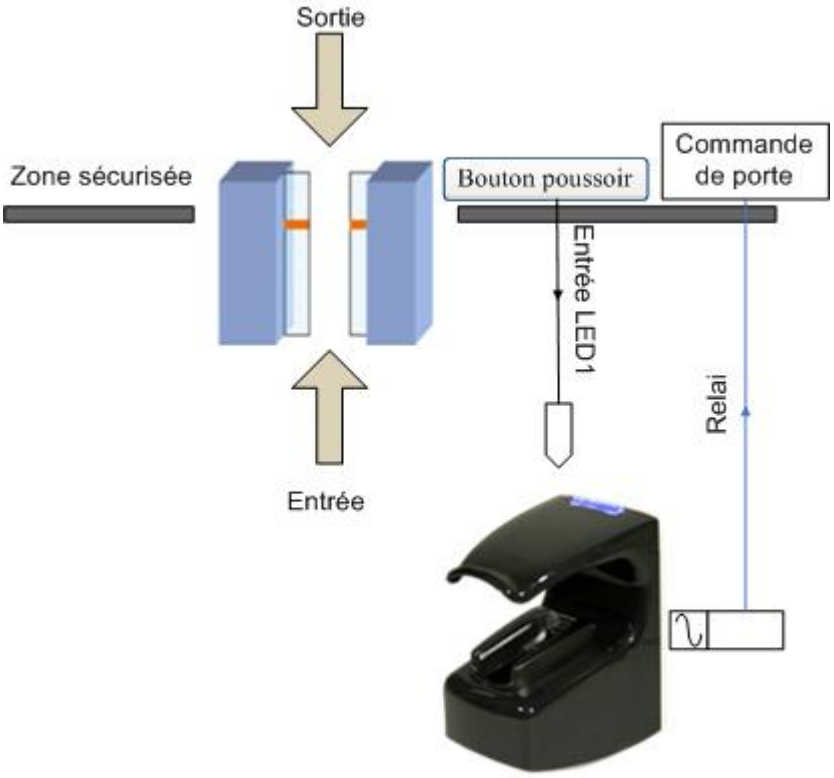


Figure 41: Relais interne activé par signal LED 1

Clé d'activation

Cette fonction est conditionnée à une seule clé de configuration.

Commande du relais du MorphoAccess® par le signal LED1	
app/relay/external control by LED1 = 0	Inhibé (par défaut)
app/relay/external control by LED1 =1	Activé

Journalisation des demandes d'accès (logs)

Description

Lorsque cette fonction est active, le terminal créé un enregistrement dans un fichier journal interne, pour chaque demande d'accès. Chaque enregistrement contient :

- la date et l'heure de la création de l'enregistrement (c'est-à-dire, l'heure de fin de traitement de la demande d'accès)
- l'identifiant de l'utilisateur (s'il est connu)
- le type de processus de contrôle de droit d'accès exécuté (identification, authentification avec contrôle biométrique,…)
- le résultat du contrôle effectué par le terminal: accès autorisé ou interdit, et pourquoi l'accès est refusé (utilisateur non reconnu, hors de la plage horaire autorisée, …).
- D'autres valeurs utilisées pour des statistiques de fonctionnement

Le format des enregistrements du fichier journal est décrit dans le document *MorphoAccess® Host System Interface Specifications*.

Gestion du fichier journal

Trois commandes sont disponibles pour la gestion du fichier journal :

- Une commande permet de lire l'état de la journalisation (active/inactive, nombre d'enregistrements dans le fichier journal)
- Une commande permet de lire les enregistrements du fichier journal (Avec le logiciel « *MA GetLog* », l'utilisation de la commande lecture efface automatiquement le journal.)
- Une commande permet d'effacer le fichier journal

Ces commandes sont décrites dans le document *MorphoAccess® Host System Interface Specifications*.

Capacité du fichier journal

La capacité du fichier est configurable jusqu'à 65 000 enregistrements (8 000 par défaut).

Lorsque le fichier est plein, l'enregistrement s'interrompt automatiquement et, suivant la configuration du terminal, un message d'avertissement peut être envoyé à un système distant.

Le format de ce message d'alarme est décrit dans le document *MorphoAccess® Remote Messages Specifications*.

Clé d'activation

La création dans le fichier journal d'un enregistrement par demande d'accès est conditionnée par une seule clé de configuration.

Autorisation de création d'un enregistrement pour chaque demande d'accès.	
app/log file/enabled = 1	Autorisé (valeur par défaut)
app/log file/enabled = 0	Inhibé

Envoi du message résultat de contrôle d'accès

Présentation

Après la vérification des droits de contrôle d'accès, le terminal MorphoAccess® peut envoyer un message contenant le résultat de cette vérification. Ce message est généralement destiné à un système distant comme un contrôleur d'accès central, et il peut être envoyé par différent ports, en utilisant un protocole à choisir.

Ce message peut être utilisé pour différentes actions, suivant le rôle du récepteur dans le système de contrôle d'accès : simple journalisation des demandes d'accès (pas de réponse attendue), ou réalisation de vérification supplémentaire des droits d'accès (réponse attendue : accès autorisé ou accès refusé).

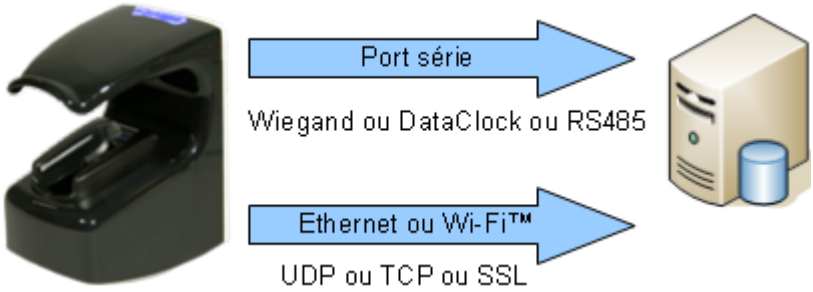


Figure 42: Envoi de résultat de contrôle d'accès à un système distant

Le format des messages et le protocole d'échange avec le système distant sont décrits dans le document *MorphoAccess® Remote Messages Specifications*.

La fonction LED IN permet d'attendre une réponse positive du système distant avant d'autoriser l'accès.

Port disponibles et protocoles pris en charge

Le terminal MorphoAccess® VP peut envoyer le message de résultat de contrôle d'accès local à un système distant, en utilisant plusieurs ports et plusieurs protocoles:

- Port série : protocole Wiegand ou DataClock, ou RS485
- Port Ethernet ou Wi-Fi™ : protocole UDP ou TCP ou SSL

Ces différentes possibilités sont détaillées dans les sections suivantes.

Port série (sortant uniquement)

Choix du protocole

Il n'y a qu'un seul port série, et il faut donc choisir un seul protocole à utiliser parmi ceux supportés : Wiegand, DataClock, ou RS485.

Protocole Wiegand

La trame Wiegand ne comprend pas d'autres données utiles que l'identifiant utilisateur (qui doit être une valeur numérique).

Par défaut, le message est envoyé uniquement lorsque le résultat du contrôle d'accès local est positif (accès autorisé), mais ce message peut également être envoyé lorsque le résultat est négatif (accès refusé). Dans ce cas, l'identifiant de l'utilisateur est remplacé par un code d'erreur indiquant la cause du refus d'accès.

L'émission de ce message est conditionnée à une clé de configuration.

Envoi du message de résultat de contrôle local sur le port série, en Wiegand	
app/send ID wiegand/enabled = 1	Autorisé
app/send ID wiegand/enabled = 0	Inhibé

Le format de la trame Wiegand sortante est configurable par l'utilisateur.

Protocole DataClock

Même commentaire que pour la trame Wiegand.

L'émission de ce message est conditionnée à une clé de configuration.

Envoi du message de résultat de contrôle local sur le port série, en DataClock	
app/send ID dataclock /enabled = 1	Autorisé
app/send ID dataclock /enabled = 0	Inhibé

Protocole RS485

Un message est envoyé quel que soit le résultat du contrôle d'accès local, et il contient davantage d'informations qu'en Wiegand ou en DataClock.

Le message envoyé contient l'identifiant utilisateur (s'il est disponible), la date et l'heure, le résultat du contrôle d'accès local (autorisé, refusé).

L'émission de ce message est conditionnée à une clé de configuration.

Envoi du message de résultat de contrôle local sur le port série, en RS485	
app/send ID serial /enabled = 1	Autorisé
app/send ID serial /enabled = 0	Inhibé
app/send ID serial/mode = 485	Protocole RS485

Port Ethernet

Choix du protocole

Le message de résultat de contrôle d'accès, peut être envoyé sur le port Ethernet, en utilisant l'un des protocoles suivant : UDP ou TCP ou SSL.

Protocole UDP

Même commentaire que pour le protocole RS485

Envoi du message de résultat du contrôle d'accès en UDP sur le port Ethernet	
app/send ID UDP/enabled = 1	Autorisé
app/send ID UDP /enabled = 0	Inhibé

Protocole TCP

Même commentaire que pour le protocole RS485

Envoi du message de résultat du contrôle d'accès en TCP sur le port Ethernet	
app/send ID ethernet /mode = 0	Inhibé
app/send ID ethernet /mode = 1	UDP
app/send ID ethernet /mode = 2	TCP

Protocole SSL

Pour obtenir des détails sur le protocole SSL, consulter le document SSL Solution for MorphoAccess®.

Port Wi-Fi™

A la place d'une connexion Ethernet, le terminal peut être connecté à l'aide d'une connexion sans fil Wi-Fi™ b/g. Merci de consulter le paragraphe Configuration du réseau Wi-Fi™ pour plus d'informations.

Le format de message et les protocoles pris en charge sont les mêmes que dans le cas d'une liaison Ethernet: UDP, TCP ou SSL.

Attention : un terminal ne peut être connecté via une connexion Ethernet et Wi-Fi™ en même temps.

Remarque concernant la dérive de l'horloge du terminal

Le message envoyé via le protocole IP et RS485 inclut la date / l'heure de l'opération. L'horloge du terminal dispose d'un écart de temps typique de +/- 4 secondes par jour à + 25 °C.

À + 50 °C, l'écart de temps peut aller jusqu'à 8 secondes par jour.

Pour une application nécessitant une précision temporelle (telle que le protocole SSL, ou DESFire®), l'horloge du terminal MorphoAccess® doit être synchronisée régulièrement avec une horloge externe (à l'aide de la commande ILV appropriée ou de l'application MorphoEnroll).

Fonctionnalité LED IN

Description

Lorsque cette fonction est activée, le terminal attend une réponse d'un système distant (par exemple un contrôleur d'accès), avant d'autoriser l'accès définitif. En l'absence de réponse, l'accès est refusé, même si le contrôle biométrique est positif.

Cette fonction est à utiliser en complément de la fonction Envoi du message résultat de contrôle d'accès.

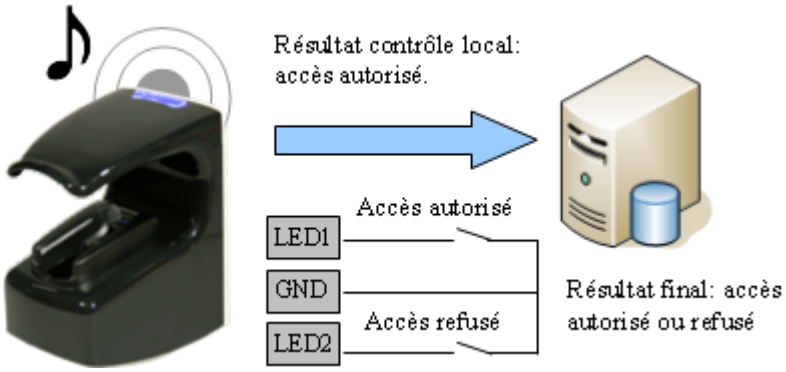


Figure 43 : Fonctionnalité LED IN

Merci de consulter le document MorphoAccess® VP Series Manuel Installation pour plus d'information sur le raccordement de cette interface.

Procédure

- Si l'utilisateur est reconnu, le terminal envoie l'identifiant de l'utilisateur au contrôleur d'accès central (dans le message de résultat de contrôle d'accès).
- Le terminal se met alors en attente, pendant un délai réglable, de la fermeture d'un contact entre LED1 et GND ou entre LED2 et GND.
- Pendant ce temps, le contrôleur effectue son propre contrôle des droits d'accès de l'utilisateur identifié.
- Suivant le résultat de ce contrôle, le contrôleur d'accès ferme le contact connecté aux bornes LED1/GND pour autoriser l'accès, ferme le contact connecté aux bornes LED2/GND pour refuser l'accès. En cas de dépassement du délai d'attente, l'accès est également refusé.
- Le terminal indique alors le résultat du contrôle d'accès à l'utilisateur, puis retourne en attente d'une demande d'accès dès que les signaux LED1 et LED2 sont revenus dans leur état par défaut

Le contrôleur d'accès ne gère pas les signaux LED1 et LED2

Lorsque le contrôleur d'accès ne dispose d'aucun contact de relais pour donner sa réponse au terminal MorphoAccess®, alors la décision d'émettre un signal d'autorisation ou de refus d'accès est prise par un autre moyen. Soit le terminal MorphoAccess® décide seul, ou bien attend la réponse du contrôleur d'accès sur le réseau local en TCP, ou sur le port série en RS422.

Il est fortement conseillé de désactiver la fonction LED IN, pour éviter toute interférence sur le fonctionnement du terminal MorphoAccess®,

Le contrôleur d'accès ne gère que le signal LED1

Lorsque le contrôleur ne dispose que d'un seul contact de relais, et que celui-ci est dédié à la réponse « accès autorisé », celui-ci doit être connecté entre les bornes LED1 et GND. La mise à l'état bas de la borne LED1 (par fermeture du contact entre LED1 et GND), par le contrôleur indique une réponse « accès autorisé ».

Le terminal MorphoAccess® utilise le dépassement du délai d'attente d'un signal sur la borne LED1 (et sur la borne LED2) comme réponse « accès refusé ».

Afin de réduire au maximum le temps d'attente de l'utilisateur, la valeur du délai d'attente de la réponse du contrôleur, doit être réglée à une valeur légèrement supérieure au temps de réponse maximal du contrôleur.

Attention : si la borne LED 2 est connectée, elle doit être maintenue constamment à l'état haut.

Le contrôleur d'accès gère les signaux LED1 et LED2

Lorsque le contrôleur propose un contact de relais pour chacune des réponses possibles, alors :

- le contact « accès autorisé » doit être raccordé aux bornes LED1 et GND
- le contact « accès refusé » doit être connecté aux bornes LED2 et GND du terminal.

Le terminal MorphoAccess® considère que :

- La réponse du contrôleur est « accès autorisé », si celui-ci met la borne LED 1 à l'état bas (par fermeture du contact entre les bornes LED1 et GND) et laisse le signal LED 2 à l'état haut.
- La réponse du contrôleur est « accès refusé », si celui-ci met la borne LED 2 (par fermeture du contact entre les bornes LED2 et GND) à l'état bas, et cela quelque soit l'état de la borne LED 1.

Le terminal MorphoAccess® considère également que la réponse du contrôleur est « accès refusé » en cas de dépassement du délai d'attente d'un état bas sur la borne LED1 ou sur la borne LED2.

Clé d'activation

Cette fonction est activée par une seule clé de configuration.

Activation de la fonction LED IN	
app/led IN/enabled = 0	Inhibée (par défaut)
app/led IN/enabled =1	Activée

Clé de configuration

La valeur du délai d'attente de la réponse du système distant (état bas sur la borne LED1 ou sur la borne LED2) est définie par une clé de configuration dédiée. Lorsque le délai d'attente est dépassé le terminal refuse l'accès.

LED IN délai d'attente de la réponse, en multiple de 10 ms	
app/led IN/controller ack timeout	300 (0 to 268435455)

Accès suivant la plage horaire (Time Mask)

Description

Le terminal MorphoAccess® dispose d'une fonction permettant d'interdire l'accès à un utilisateur normalement autorisé, en fonction de l'heure à laquelle l'accès est demandé.

Un exemple typique d'utilisation de cette fonction est d'autoriser pour une même personne, l'accès pendant la journée et les jours ouvrables, et l'interdire la nuit et en fin de semaine.

Cette fonction n'est disponible que pour le mode identification.

L'application MorphoEnroll est compatible avec cette fonction.

Pour plus d'informations sur cette fonction, merci de consulter le document *MorphoAccess® Host System Interface Specifications*.

Base biométrique

Pour utiliser cette fonctionnalité, la base de données locale doit avoir été créée avec un champ supplémentaire spécifique.

Chaque utilisateur peut avoir un masque différent des autres utilisateurs.

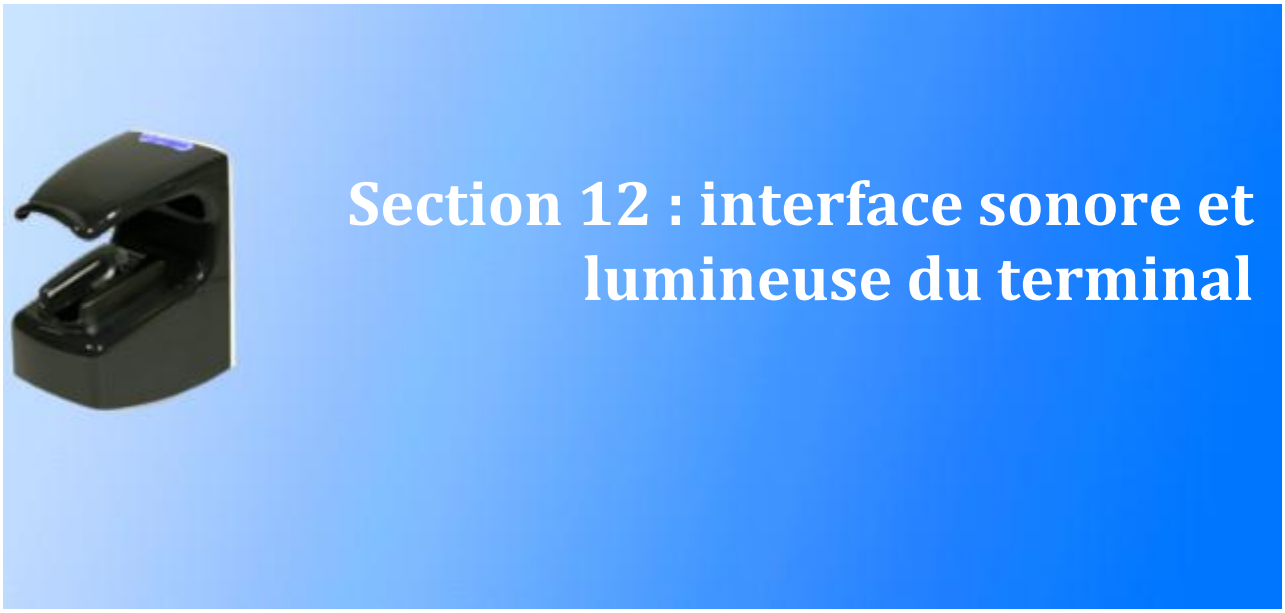
Le masque de temps est défini par des intervalles de 15 minutes sur une semaine. Chacun des 84 intervalles (de 15 mn) doit être défini individuellement, comme une période d'accès autorisé ou d'accès refusé.

Attention : Si ce champ n'existe pas, l'activation de cette fonctionnalité interdit l'accès à tous les utilisateurs.

Clé d'activation

Cette fonction est activée par une seule clé de configuration

Ajout du contrôle d'accès sur la base de la plage horaire	
app/modes/time mask = 1	Activé
app/modes/time mask = 0	Inhibé (par défaut)



Section 12 : interface sonore et lumineuse du terminal

IHM Lumineuse et sonore

Description du signal émis par la LED d'état

Clignotement: 0,5 seconde allumée, puis 1 seconde éteinte

Exemple:

Clignotement bleu	

Clignotement rapide: 0,5 seconde allumée, puis 0,5 seconde éteinte.

Exemple:

Clignotement jaune rapide	

Clignotement lent: 1 seconde allumée, 1 seconde éteinte

Exemple:

Clignotement rouge lent	

Signal sonore

Le volume du signal sonore peut être réglé avec une clé de configuration dédiée.

Level of the audible signal	
app/GUI/volume = 0	Muet
app/GUI/volume = 1 à 10	Réglage progressif (de faible à fort, 10 par défaut)

Tables des signaux

Etat du terminal

Etat	Capteur biométrique	LED d'état	Son
En attente d'un doigt ou d'une carte	Eteint	Bleu fixe	-
En attente d'un doigt ou acquisition du doigt en cours (mode authentification, après lecture d'une carte)	Vert fixe	Eteint	-
Acquisition du doigt en cours (mode identification, après détection d'un doigt)	Vert fixe	Bleu fixe	-
Mauvais positionnement du doigt	Eteint	Clignotement jaune	-
Doigt retiré trop tôt	Eteint	Jaune	-
Pas de base ou base vide	Eteint	Clignotement Jaune	-
La clé mémoire USB peut être retirée	Eteint	Clignotement rapide Cyan	-
Commande distante en cours	Eteint	Clignotement Magenta	-
Mise à jour du logiciel du capteur biométrique en cours	Eteint	Clignotement Magenta	-
Capteur en erreur	Eteint	Clignotement Rouge	-

Résultat du contrôle d'accès

Evénement	Capteur biométrique	LED d'état	Son
Accès autorisé	Eteint	Flash Vert	Note aigüe
Accès refusé	Eteint	Flash rouge	Note grave

Enrôlement

Evénement	Capteur biométrique	LED d'état	Son
Attente d'un doigt ou acquisition en cours	VERT fixe	Clignotement magenta rapide	-
Acquisition en cours	VERT fixe	Clignotement magenta rapide	
Pose courante - Acquisition terminée (mais pas la séquence d'enrôlement)	VERT fixe	Clignotement magenta rapide	Note aigüe
Capture courante terminée - Retirer le doigt pour passer à la suivante	VERT fixe	Eteinte 1 sec. Puis clignotement magenta rapide	
Doigt courant – Acquisition terminée (mais pas la séquence d'enrôlement)	VERT fixe	Flash vert 0,5 seconde	-
Enrôlement terminé	Eteint	Flash vert 1 seconde	-
Enrôlement terminé – Enregistrement des données biométriques en cours	Eteint	Clignotement magenta rapide	-
Mauvais positionnement du doigt	VERT fixe	Clignotement jaune rapide	-

Etat du terminal

Mode Identification, Authentification ou Multi-facteurs : en attente d'un doigt ou d'une carte

En mode Identification le terminal est en attente de la pose d'un doigt sur le capteur biométrique.

En mode Authentification le terminal est en attente d'une carte.

En mode multi-facteurs, le mode identification et l'un des modes authentification sont activés en même temps.

Rétro-éclairage capteur	Eteint
LED d'état	Fixe bleue 
Son	Aucun

Mode authentification, après présentation d'une carte : Attente d'un doigt ou Acquisition des données biométriques du doigt en cours

Après lecture d'une carte, le terminal émet ce signal pendant l'attente d'un doigt ou lorsqu'il est en train d'acquérir les données biométriques du doigt placé sur le capteur. Ne pas retirer le doigt tant que ce signal est émis.

Rétro-éclairage capteur	VERT fixe
LED d'état	Eteinte
Son	Aucun

Identification : Doigt détecté, Acquisition des données biométriques du doigt en cours

Après détection d'un doigt sur le capteur, le terminal émet ce signal pendant toute la phase d'acquisition des données biométriques du doigt placé sur le capteur. Ne pas retirer le doigt tant que ce signal est émis.

Rétro-éclairage capteur	VERT fixe
LED d'état	Fixe bleue 
Son	Aucun

Identification ou Authentification : base vide ou absente

Ce signal est émis lorsque le mode activé nécessite une base (mode identification, ou mode authentification avec données dans la base), et que celle-ci n'est pas crée ou est vide.

Rétro-éclairage capteur	Eteint
LED d'état	Clignotement jaune lent 
Son	Aucun

Mode proxy : en attente d'un ordre du système distant

Lorsque le terminal est en mode proxy, et en attente d'un ordre du système distant, il n'y a aucun signal local.

Rétro-éclairage capteur	Eteint
LED d'état	Eteint
Son	Aucun

Doigt mal placé

Le terminal émet ce signal lorsque le placement du doigt sur le capteur n'est pas optimal. Retirez le doigt et respectez les règles de placement citées dans la section Annexe 1 : Règles de positionnement du doigt.

Rétro-éclairage capteur	VERT fixe
LED d'état	Clignotement jaune rapide 
Son	OFF

Le capteur biométrique ne démarre pas

Ce signal est émis lorsque le terminal constate une erreur de démarrage du capteur biométrique. Si le problème persiste, après plusieurs démarrages du terminal, veuillez contacter votre revendeur de produits Morpho.

Rétro-éclairage capteur	Eteint
LED d'état	Clignotement rouge lent.
Son	Off

Maintenance : le terminal est en cours de configuration

Ce signal indique qu'une opération de configuration est en cours, que ce soit par TCP ou par clé USB. L'opération en cours peut être l'une des suivantes : gestion de la base biométrique, modification d'une clé de configuration, gestion du fichier journal, etc…

Dans cet état, le terminal ignore les demandes d'accès.

Rétro-éclairage capteur	Eteint
LED d'état	Clignotement magenta lent
Son	Aucun

Maintenance : mise à jour du logiciel embarqué du capteur biométrique

Ce signal est émis lorsque la mise à jour du logiciel embarqué du capteur biométrique est en cours. Cette mise à jour ne se produit qu'au démarrage du terminal, et uniquement après une mise à jour du logiciel embarqué du terminal.

Rétro-éclairage capteur	Eteint
LED d'état	Clignotement magenta lent
Son	Aucun

Mode Maintenance: la clé mémoire USB peut être retirée

Ce signal est émis lorsque la clé mémoire USB utilisée pour configurer le terminal peut être retirée du port USB. La clé mémoire USB doit être retirée pour que le processus de maintenance puisse se terminer.

Rétro-éclairage capteur	Eteint
LED d'état	Clignotement cyan rapide
Son	Deux bips moyens consécutifs

Intrusion ou arrachement détecté

Ce signal est émis lorsque le terminal a détecté le retrait de la trappe inférieure, ou un écart significatif avec son support mural.

Rétro-éclairage capteur	Non significatif
LED d'état	Clignotement rouge lent
Son	Succession de bips grave

Modification de la taille du journal de transaction en échec

Rétro-éclairage capteur	Non significatif
LED d'état	Flash rouge 2 sec.
Son	Bip grave 1 sec.

Résultat de la demande d'accès

Mode Identification ou Authentification - Accès autorisé

L'utilisateur est reconnu et l'accès est autorisé.

Rétro-éclairage capteur	Non significatif
LED d'état	Flash vert 1 sec.
Son	Bip aigu 1 sec.

Mode Identification ou Authentification - Accès refusé

L'utilisateur n'est pas reconnu, ou l'accès n'est pas autorisé (y compris par la fonction plage horaire, ou par le contrôleur d'accès central).

Rétro-éclairage capteur	Non significatif
LED d'état	Flash rouge 1 sec.
Son	Bip grave 1 sec.

Authentification - Timeout attente de pose de doigt sur le capteur

Mode Authentification uniquement: aucun doigt n'a été détecté sur le capteur pendant la durée maximale autorisée (timeout).

Rétro-éclairage capteur	Non significatif
LED d'état	Flash rouge 1 sec.
Son	Bip grave 1 sec.

Doigt retiré trop tôt

Le terminal émet ce signal lorsque le doigt à été retiré alors que l'acquisition des données biométriques n'était pas terminée.

Rétro-éclairage capteur	Eteint
LED d'état	Flash jaune 1 sec.
Son	Aucun

Enrôlement

Attente d'un doigt

La séquence d'enrôlement est lancée, le terminal attend que l'utilisateur pose un doigt sur le capteur biométrique.

Rétro-éclairage capteur	VERT fixe
LED d'état	Clignotement magenta rapide
Son	Aucun

Acquisition en cours

L'utilisateur a posé son doigt sur le capteur biométrique, et il doit attendre la fin de l'acquisition (signalée par l'événement Acquisition terminée).

Rétro-éclairage capteur	VERT fixe
LED d'état	Clignotement magenta rapide
Son	Aucun

Pose courante - Acquisition terminée (mais pas la séquence d'enrôlement)

L'acquisition courante est terminée, l'utilisateur peut retirer son doigt.

Rétro-éclairage capteur	VERT fixe
LED d'état	Clignotement magenta rapide
Son	**Bip aigu 0,5 sec**.

Capture courante terminée - Retirer le doigt pour passer à la suivante

La capture courante est terminée, l'utilisateur est invité à retirer le doigt qu'il a laissé posé sur le capteur. La capture suivante ne se fera pas tant que le doigt n'aura pas été retiré.

Rétro-éclairage capteur	VERT fixe
LED d'état	Eteinte 1 sec. Puis clignotement magenta rapide 
Son	Aucun

Doigt courant – Acquisition terminée (mais pas la séquence d'enrôlement)

L'acquisition du doigt courant est terminée avec succès, et l'utilisateur vient de retirer son doigt. Si un autre doigt reste à acquérir, le terminal émet ensuite le signal Attente d'un doigt.

Rétro-éclairage capteur	VERT fixe
LED d'état	Flash vert 500 ms. 
Son	Aucun

Enrôlement terminé

La séquence d'enrôlement est terminée avec succès. Suivant la durée nécessaire au processus d'enregistrement des données biométriques, le terminal peut émettre le signal Enrôlement terminé – Enregistrement des données biométriques en cours.

Rétro-éclairage capteur	Eteint
LED d'état	Flash vert 1s 
Son	Aucun

Enrôlement terminé – Enregistrement des données biométriques en cours

La séquence d'enrôlement est terminée, l'enregistrement des données biométriques est en cours.

Rétro-éclairage capteur	Eteint	
LED d'état	Clignotement magenta rapide	
Son	Aucun	

Section 13: Accessoires, licences logicielles et applications PC

Accessoires et licences logicielles compatibles

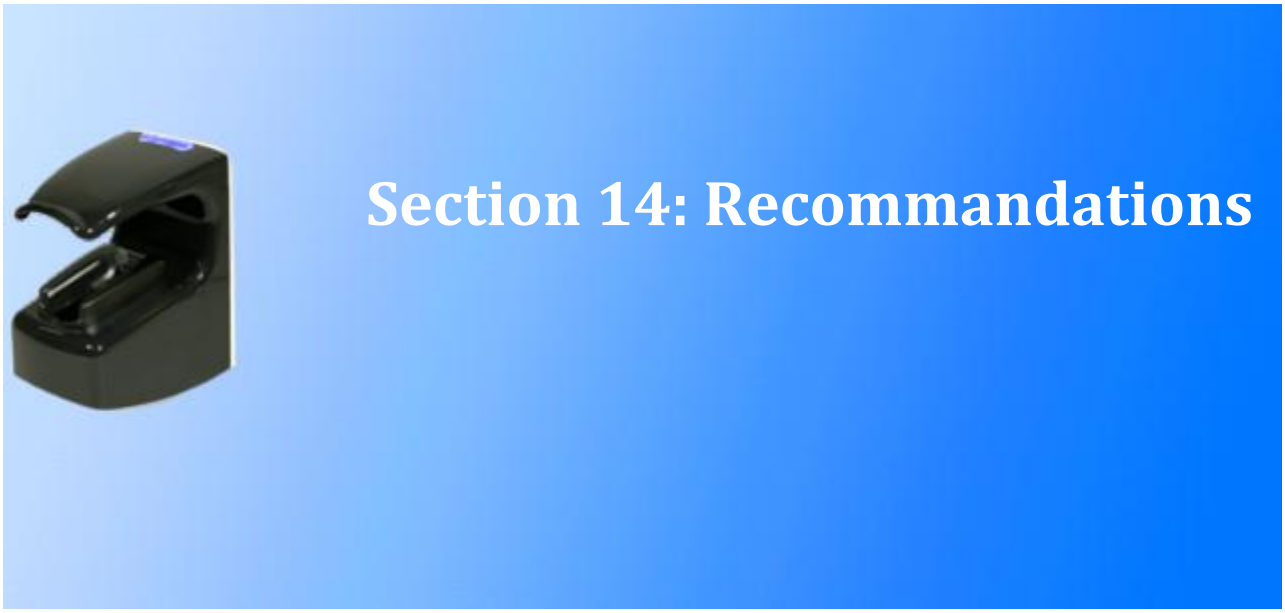
Les éléments suivants peuvent être commandés directement auprès de Morpho ou auprès d'un distributeur officiel afin de bénéficier de toutes les fonctionnalités de votre terminal MorphoAccess® VP :

- Bloc d'alimentation électrique
- Cartes à puce sans contact : MIFARE® 4K ; DESFire® 2K, 4K ou 8K
- PACK MA WI-FI, contenant une clé USB Wi-Fi™ et une licence Wi-Fi™ pour activer la fonction Wi-Fi™ du terminal
- Licence MA 10K USERS, permettant d'augmenter la taille maximale autorisée lors de la création de la base interne, de 5.000 à 10.000 enregistrements utilisateurs (2 doigts par enregistrement).

Applications PC compatibles

Les terminaux de la Série MorphoAccess® VP sont totalement compatibles avec :

- l'application d'enrôlement MorphoEnroll
- le protocole bas niveau à base de commandes ILV
- le kit de développement logiciel Morpho Integrator's Kit (MIK) (à venir)


Section 14: Recommandations

Avertissement

Le fabricant ne peut être tenu responsable en cas de non-respect des recommandations ci-dessous ou en cas d'utilisation inappropriée du terminal.

Précautions générales

- Ne pas essayer de réparer le terminal soi-même. Le fabricant ne peut être tenu responsable de tout dommage / accident survenant suite à des tentatives de réparation des composants. Tout travail effectué par un personnel non autorisé annulera la garantie.
- Ne pas exposer le terminal à des températures extrêmes.
- Utiliser le terminal avec les accessoires d'origine. Toute tentative d'intégrer des accessoires non approuvés pour le terminal annulera la garantie.
- En raison des risques de décharge électrostatique, et en fonction de l'environnement, éviter les tapis synthétiques dans la zone où le terminal a été installé.

Zones contenant des combustibles

Il est fortement déconseillé d'installer le terminal à proximité de stations-services, d'installations de traitement de pétrole ou de toute autre installation contenant des gaz ou matières inflammables ou combustibles.

Précautions spécifiques relatives aux terminaux équipés d'un lecteur de cartes à puce sans contact

Il est recommandé d'installer les terminaux équipés d'un lecteur de cartes à puce sans contact à une certaine distance (> 30 cm) d'éléments métalliques tels que des fixations en fer ou des portes d'ascenseur. Les performances, du point de vue de la distance de lecture des badges sans contact, diminueront lorsque des éléments métalliques seront proches du terminal.

Connexion Ethernet

Il est recommandé d'utiliser un câble blindé de catégorie 5 (120 ohms). Il est également fortement recommandé d'insérer une unité répétitrice tous les 90 m.

Faire extrêmement attention lors du branchement du câble Ethernet au bornier du terminal étant donné qu'un branchement de basse qualité peut fortement affecter la sensibilité du signal Ethernet.

Il est recommandé de brancher Rx+ et Rx- avec la même paire torsadée (et procéder de même avec Tx+ / Tx- et l'autre paire torsadée).

Synchronisation date / heure

Si vous souhaitez utiliser le terminal pour une utilisation nécessitant une haute précision en termes d'heure, nous vous recommandons de synchroniser régulièrement l'heure de votre terminal avec une horloge externe.

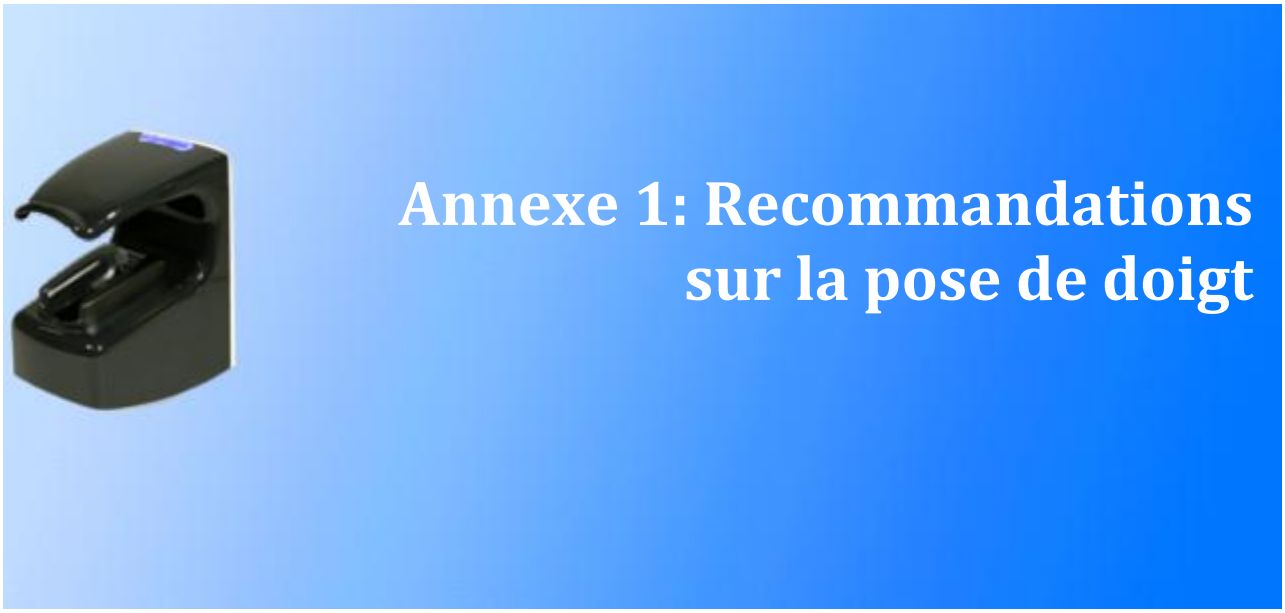
L'horloge du terminal dispose d'un écart de temps typique de +/- 40.10^{-6} (ppm) à + 25 °C. Soit, +/- 4 secondes par jour.

À + 45 °C, l'écart de temps peut aller jusqu'à +/- 8 secondes par jour.

Précautions de nettoyage

Il est recommandé d'utiliser un chiffon sec pour nettoyer le terminal, en particulier le capteur biométrique.

Il est interdit d'utiliser des liquides acides, de l'alcool ou des matières abrasives.


Annexe 1: Recommandations
sur la pose de doigt

Zones les plus riches en données biométriques

Les zones les plus riches en données biométriques sont différentes suivant la nature de la donnée biométrique :

- **Empreinte digitale** : la zone la plus utile se trouve autour du centre de la 1ère phalange du doigt.
- **Réseau veineux** : la zone intéressante se situe entre la 1ère et la 3ème phalange du doigt.

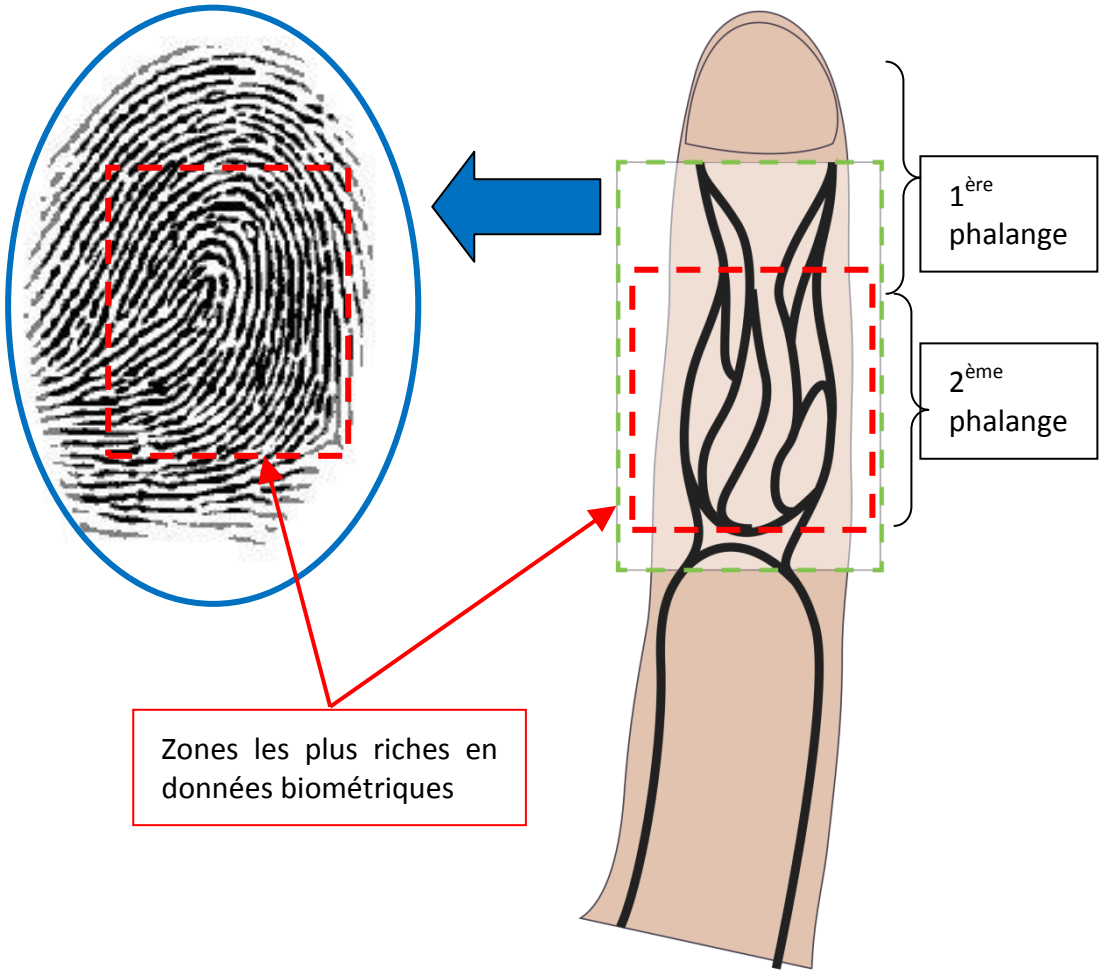


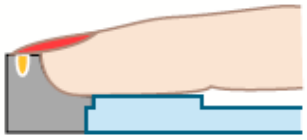
Figure 44 : Zones les plus riches en données biométriques

Le capteur est conçu de manière à ce que lorsque le bout du doigt est en contact avec le guide creux arrondi :

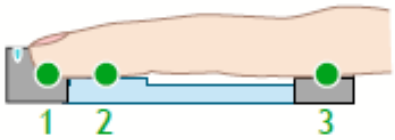
- La zone centrale de la 1ère phalange est alignée avec celle de la section dédiée à la capture d'empreinte digitale
- La 2ème phalange se trouve en face de la section dédiée à la capture du réseau veineux du doigt.

Placement du doigt

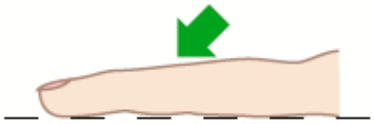
Bonne position



- Placer le bout du doigt en contact avec le guide creux arrondi (1).
- Lorsque l'ongle est particulièrement long, le faire passer au dessus du guide de bout de doigt de façon à ce que ce soit bien le bout de doigt qui soit en contact avec le guide creux (1) et pas l'extrémité de l'ongle.



- Laisser le bout du doigt en contact avec le guide creux arrondi (1).
- S'assurer que l'empreinte digitale est bien en contact avec la surface optique transparente (2).
- Placer la base du doigt dans le guide de positionnement à l'autre bout (3).
- Laisser reposer la paume de la main sur la coque du terminal



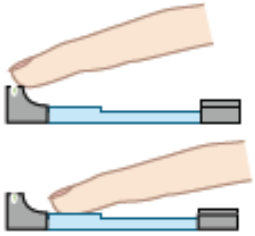
- Garder le doigt bien en ligne.

Figure 45 : Positions de doigt recommandées

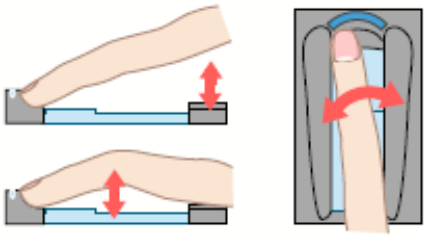
Afin de garantir une bonne qualité d'acquisition, merci de laisser le doigt sur le capteur biométrique jusqu'à ce que le retro-éclairage s'éteigne.

Mauvaise position

Les figures ci-dessous montrent les positions de doigt à éviter.



- Ne pas poser le bout du doigt sur le dessus du guide de bout de doigt.
- Ne pas poser le bout du doigt sur la surface du capteur : il doit être en contact avec le guide creux arrondi.



- Ne pas laisser le doigt en l'air.
- Ne pas plier le doigt.
- Ne pas incliner le doigt : il doit être parallèle aux parois du capteur.

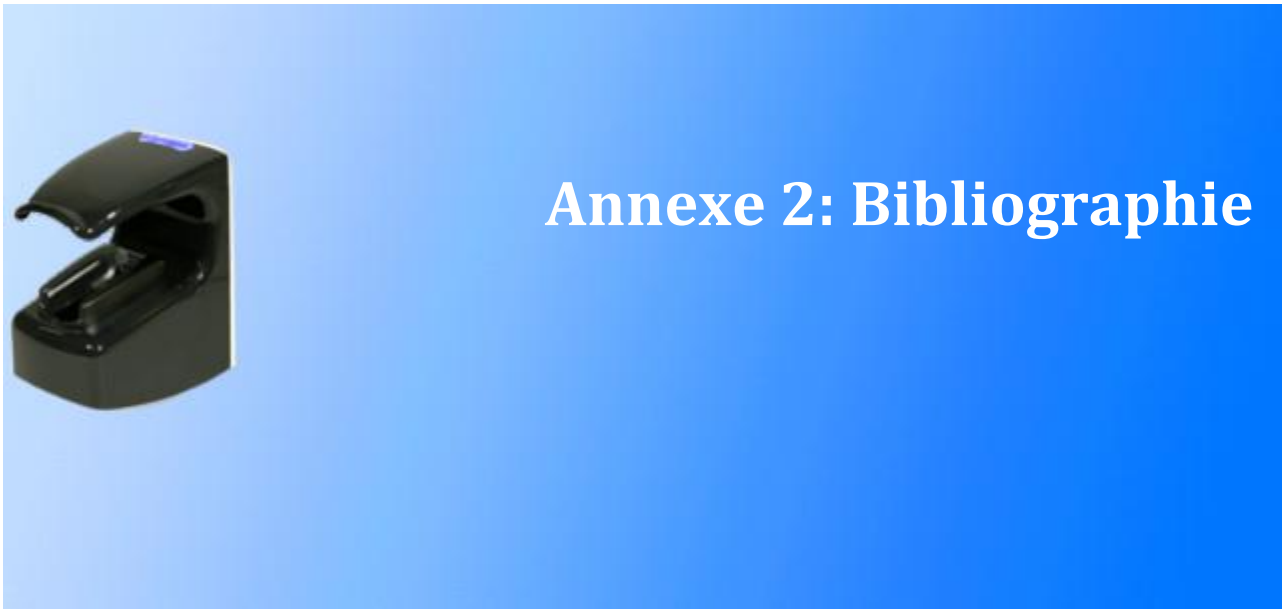
- Ne pas rouler le doigt.
- Ne pas plier le doigt vers le haut.
- Ne pas plier le doigt vers le bas.

Figure 46 : Positions de doigt déconseillées

Etat du doigt

Merci de suivre les recommandations ci-dessous afin d'améliorer la qualité de l'acquisition :

- Essuyez le doigt s'il est trop humide
- Réchauffer le doigt s'il est froid ou sec
- Humidifier un peu le doigt s'il est sec
- Nettoyer le doigt s'il est sale
- Enlevez les bandages et rubans adhésifs s'ils masquent l'empreinte digitale ou la 2ème phalange du doigt.
- Ne pas appuyer trop fort et ne pas raidir le doigt, afin d'éviter la constriction de vaisseaux sanguins.



Annexe 2: Bibliographie

Comment obtenir la dernière version des documents

Les documents dans leur dernière version peuvent être obtenus sur un CD/ROM, ou bien être téléchargés depuis notre site Web à l'adresse suivante :

www.biometric-terminals.com

(Identifiant et mot de passe requis).

Pour obtenir votre identifiant, merci de nous envoyer un message à l'adresse suivante.

hotline.biometrics@t.my-technicalsupport.com

Documents relatifs au terminal MorphoAccess®

Documents relatifs à l'installation

MorphoAccess® VP Series Guide d'Installation, réf. SSE-00000 83014

Ce document décrit la procédure d'installation physique du terminal, les interfaces électriques et les procédures de connexion. Ce document est en langue française.

Documents destinés à l'administrateur

MorphoAccess® Parameters Guide, réf. SSE-0000062458

Ce document contient la description complète de tous les paramètres de configuration du terminal. Ce document est en langue anglaise.

SSL Solution for MorphoAccess®, réf. SSE-0000069007

Ce document décrit le déploiement de la Solution SSL pour le MorphoAccess®. Ce document est en langue anglaise.

MorphoAccess® Terminal License Management, réf. SSE-0000066855

Ce document explique comment charger, et lire les licences dans un terminal MorphoAccess®. Ce document est en langue anglaise.

MorphoAccess® Station d'enrôlement- Guide utilisateur, réf. SSE-0000035834

Le chapitre 15 « Configurer les paramètres réseaux d'un terminal MorphoAccess® » décrit comment configurer les paramètres réseau (filaire ou Wi-Fi™), d'un terminal MorphoAccess® en utilisant l'application MATM. Ce document est en langue française.

Documents destinés au développeur

MorphoAccess® Host System Interface Specifications, réf. SSE-0000056821

Ce document contient la description complète de toutes les commandes acceptées par un terminal MorphoAccess®. Ce document est en langue anglaise.

MorphoAccess® Contactless Card Specifications, réf. SSE-0000062610

Ce document décrit les caractéristiques des cartes sans contact gérées par un terminal MorphoAccess®. Ce document décrit également le format des données stockées sur la carte. Ce document est en langue anglaise.

MorphoAccess® Remote Messages Specification, réf. SSE-0000062580

Ce document décrit le format des messages envoyés par le terminal, vers un système distant. Ce document est en langue anglaise.

Outils de support

MorphoAccess® Terminal Management User Guide, réf. SSE-0000068869

Guide d'utilisation de l'outil de configuration MATM (fonctionne uniquement avec un lien Ethernet ou Wi-Fi™). Ce document est en langue anglaise.

MorphoAccess® USB Network Tool User Guide, réf. SSE-0000043164

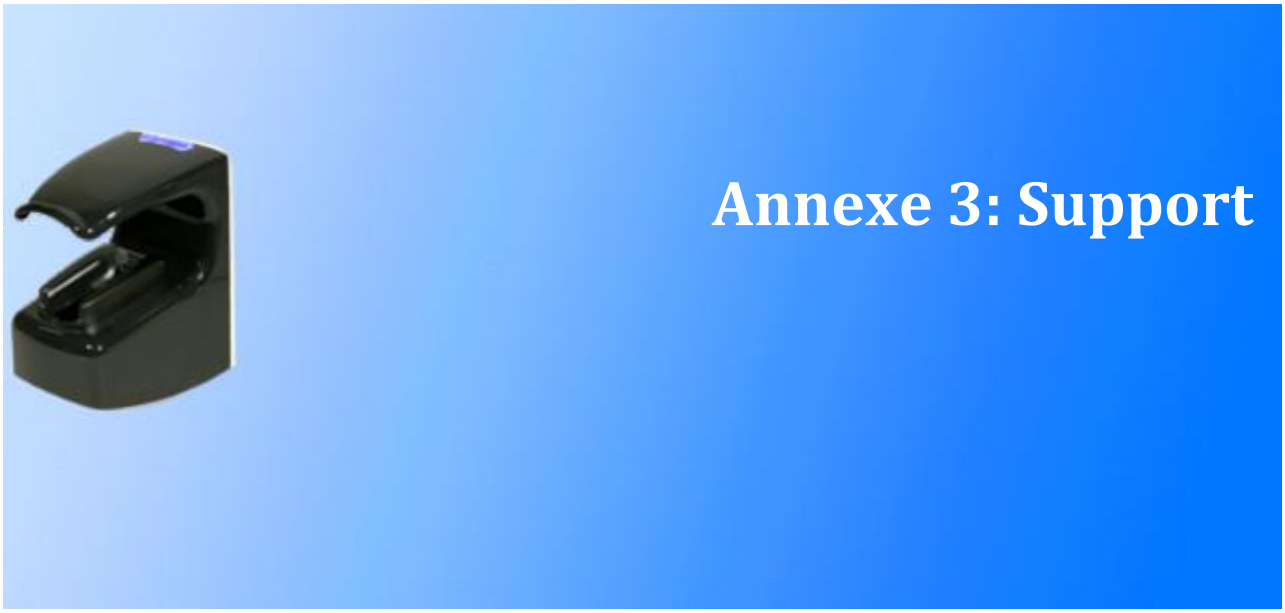
Guide d'utilisation de l'outil de configuration, via la clé mémoire USB. Ce document est en langue anglaise.

MorphoAccess® USB encoder User Guide, réf. SSE-0000050386

Guide d'utilisation de l'outil de configuration, via une clé USB.

MorphoAccess® Firmware Upgrade Guide, réf. SSE-0000038184

Ce document décrit en détail, les différentes procédures de mise à jour du logiciel embarqué (micro logiciel).



Annexe 3: Support

Dépannage

L'adresse IP du terminal est inconnue ou le terminal n'est pas joignable

Utiliser l'outil de configuration réseau par USB pour configurer une adresse réseau valide dans votre terminal. Consulter le Guide d'utilisation de l'outil de configuration réseau par USB.

Le capteur est éteint

Vérifier que la base contient au moins un enregistrement.

Vérifier que le mode d'identification est activé.

Le terminal renvoie des réponses erratiques à des commandes Ping

Vérifier le masque de sous-réseau.

Demander à l'administrateur réseau la valeur correcte.

Vérifier que chaque dispositif connecté au réseau possède une adresse IP différente.

Contacts

Service Après Vente (retour matériel)

Morpho

SAV Terminaux Biométriques

Boulevard Lénine

BP428

76805 Saint Etienne du Rouvray FRANCE

Téléphone : +33 2 35 64 53 52

Assistance client

Morpho

Support Terminaux Biométriques

18, Chaussée Jules César

95520 OSNY

France

hotline.biometrics@t.my-technicalsupport.com

Téléphone : + 33 1 58 11 39 19

(De 9 h à 18 h, heure française, du lundi au vendredi)

http://www.biometric-terminals.com/

Un identifiant (login) et un mot de passe (password) sont requis pour accéder à l'intégralité du contenu du site. Si vous n'en avez pas, envoyez-nous un message à l'adresse de messagerie ci-dessus pour les obtenir.

Merci de nous contacter par messagerie plutôt que par téléphone.

Siège social : Le Ponant de Paris
27, rue Leblanc - 75512 PARIS CEDEX 15 – France
www.morpho.com