

MorphoAccess® Série 500

Manuel Utilisateur



MA Série 500+



OMA Série 500



MA Série 500

Produced by Morpho

Copyright ©2012 Morpho

<http://www.morpho.com/>

[MorphoAccess® Série 500 - Manuel Utilisateur](#)

SSE-0000066888-07

Février 2012

Table des matières

Introduction	6
Objet du document	7
Consignes de sécurité	8
Présentation du MorphoAccess®	10
Présentation des Interfaces	11
Synoptique d'un système de contrôle d'accès physique	14
Présentation du terminal	16
Présentation du Contrôle d'Accès	18
Envoi de l'ID au Contrôleur central de Sécurité	21
Configuration du terminal	24
Assistant d'installation (EasySetup)	25
Menu d'Administration	41
Présentation de la configuration du MorphoAccess®	44
Modification d'un Paramètre - Application de configuration	46
Configuration d'un MorphoAccess® connecté à un réseau	49
Téléchargement d'une licence	53
Mise à jour du logiciel embarqué	54
Réglage du contraste	55
Application de démarrage	56
Modes autonomes (en Réseau ou déconnecté)	57
Préliminaire : ajout d'une empreinte biométrique dans la base	58
Contrôle d'Accès ou de Pointage	60
Contrôle d'accès par identification	64
Contrôle d'accès par identification (licence MA-Xtended)	66
Présentation du mode authentification sans contact	69
Authentification - empreintes biométriques sur la carte	72
Vérification du code PIN – PIN enregistré sur la carte	73
Vérification du code BIOPIN– BIOPIN enregistré sur la carte	75
Authentification - empreintes dans la base de données locale	76
Mode d'authentification imposé par la carte	80
Mode fusionné (ou mode multi-facteur)	82
Authentification avec Base Locale- ID saisi à partir du clavier	84
Authentification - ID lu sur l'entrée Wiegand / DataClock	86
Désactivation du contrôle biométrique	90
Synthèse des modes de reconnaissance	94
Réglage de la stratégie de reconnaissance	96

Réglage des paramètres de reconnaissance	97
Détection de Faux Doigt (OPTION)	98
Mode veille	100
Présentation du mode veille	101
Activation du mode veille	102
Mode proxy	103
Présentation du mode Proxy (ou mode commandé)	104
Activation du mode proxy	105
Personnalisation du terminal	106
Définition d'un contrôle horaire	107
Application multilingue	108
Affichage de l'heure	109
Exportation du Résultat du contrôle d'accès	110
Envoi de l'ID au Contrôleur central de Sécurité	111
Activation du relais	112
Fichier journal	115
Fonctionnalité LED IN	116
Fonctions de Sécurité	119
Détection d'intrusion et d'arrachement	120
Mots de passe	123
Envoi de messages	124
Principe	125
ÉVÈNEMENTS	126
Interfaces d'envoi	127
Annexes	128
Enrôlement sur terminal avec synchronisation	129
Compatibilité avec la gamme MorphoAccess® 220 / 320	131
Synthèse des modes avec carte sans Contact	133
Tags requis sur la carte sans contact	134
Documentations	135
Support	137
FAQ	138
Contacts	139

Table des illustrations

Figure 1: Face avant du terminal MorphoAccess® Série 500.....	11
Figure 2: Bornier du terminal MorphoAccess® Série 500	12
Figure 3: Architecture typique d'un système de contrôle d'accès	14
Figure 4: Synthèse des applications du terminal MorphoAccess® Série 500	17
Figure 5: Mode Identification.....	18
Figure 6: Mode authentification	19
Figure 7: Mode Proxy	20
Figure 8: Envoi du résultat du contrôle de droits d'accès.....	21
Figure 9: Configuration à distance du terminal MorphoAccess® Série 500	49
Figure 10: Outil de configuration d'un terminal MorphoAccess®	51
Figure 11: Gestion de base à distance	59
Figure 12: Identifiant utilisateur saisi au clavier	84
Figure 13: Identifiant utilisateur reçu en Wiegand	86
Figure 14: Mode Proxy	104
Figure 15: Envoi du résultat du contrôle d'accès.....	111
Figure 16: Activation du relais interne par signal LED1	113
Figure 17 : Fonctionnalité LED IN	116
Figure 18: Détection intrusion ou arrachement	120

Historique de révision

Date	Firmware	Description
Juillet 2008	2.07	Ajout d'une description concernant la date et l'heure
	2.09	Ajout de l'option juvénile
		Ajout de la fonctionnalité de pointage horaire étendu
		Ajout de la fonctionnalité Wi-Fi™
		Ajout de la MAJ des clés MIFARE dans l'assistant de configuration
		Ajout du mode de lecture du Card UID des cartes ISO/IEC 14443
Juin 2009	2.10	Ajout des séries MA 500+ et DESFire
Octobre 2009	2.11	Ajout du mode Wi-Fi™ en IP statique
		Ajout de la protection WPA-PSK
		Ajout de nouvelles langues (Arabe et Turc)
		Ajout de la fonctionnalité envoi de messages sur évènements
		Ajout de la sélection de l'application de démarrage
		Ajout des fonctionnalités offertes sur journal interne rempli
Mars 2010	2.12	Ajout des licences MA 3K USERS et MA XTENDED
Février 2011	2.13	Changement du logo et du nom de la société
Juin 2011		Amélioration description fonction LED IN
Février 2012	3.3	Ajout du support des cartes DESFire® EV1 AES
		Ajout du support de 65000 transactions

WI-FI™ est une marque déposée de la WI-FI™ Alliance

Introduction

Nous vous remercions d'avoir choisi le terminal de reconnaissance automatique d'empreintes digitales, MorphoAccess®.

Le MorphoAccess® offre une solution innovante et performante aux applications de contrôle d'accès ou de pointage à l'aide de la vérification et/ou de l'identification des empreintes digitales.

Parmi une grande variété de technologies biométriques alternatives, l'utilisation d'empreintes digitales présente des avantages significatifs : chaque empreinte constitue une signature physique inaltérable qui se développe avant la naissance et qui est préservée jusqu'à la mort. Contrairement à l'ADN, une empreinte digitale est propre à chaque individu, même pour de vrais jumeaux.

Le MorphoAccess® intègre les algorithmes de traitement de l'image et de correspondance de caractéristiques Morpho. Cette technologie est basée sur une expérience de 18 ans dans le domaine de l'identification biométrique et de la création de millions de fichiers d'identification d'empreintes digitales.

Le MorphoAccess® s'impose comme un système rapide, précis, facile à utiliser et idéal pour les applications de contrôle d'accès physique ou de pointage.

Afin de garantir l'utilisation la plus efficace de votre MorphoAccess®, nous vous recommandons de lire entièrement ce Manuel Utilisateur.

Objet du document

Ce guide s'adresse aux utilisateurs de terminaux MorphoAccess® de la série 500.


« MorphoAccess® Série 500 » est une appellation générique qui regroupe les terminaux MorphoAccess® appartenant aux séries MA 500+, OMA 500 et MA 500. La liste des produits correspondants est détaillée dans le tableau ci-dessous.

		Capteur biométrique	Lecteur de cartes sans contact		Détection de faux doigt	Outdoor (pour extérieur)
			MIFARE®	DESFire®		
Série MA 500+	MA 500+	√				
	MA 520+ D	√	√	√		
	MA 521+ D	√	√	√	√	
Série OMA 500	OMA 520 D	√	√	√		√
	OMA 521 D	√	√	√	√	√
	OMA 520	√	√			√
	OMA 521	√	√		√	√
Série MA 500	MA 500	√				
	MA 520	√	√			
	MA 521	√	√		√	

Consignes de sécurité

Informations pour l'Europe

Morpho déclare par la présente que le MorphoAccess® a été testé et jugé conforme aux normes citées ci-dessous comme prévu par la Directive CEM 89/336/CEE : EN55022 (1994)/EN55024 (1998), EN300-330 (1999) et par la Directive 73/23/CEE de basse tension amendée par 93/68/CEE : EN60950 (2000).

 Les MorphoAccess® Série 500 sont des dispositifs de Classe A. Dans un environnement résidentiel, ces dispositifs peuvent provoquer des interférences. Dans ce cas, l'utilisateur est encouragé à essayer de corriger l'interférence à l'aide de mesures appropriées telles que :

- 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,
- pour toute aide, consulter le fournisseur ou un technicien radio/TV expérimenté.


Informations pour le Canada

Ces appareils numériques de Classe A sont conformes à la norme NMB-003 du Canada.

This Class A digital apparatus complies with Canadian ICES-003.

Informations pour les USA

Responsible Party : Morpho, Le Ponant de Paris, 27, rue Leblanc – F 75512 PARIS CEDEX 15 – FRANCE

 Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 Class A of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this

equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Groupe responsable : Morpho, Le Ponant de Paris, 27, rue Leblanc – F 75512 PARIS CEDEX 15 – FRANCE



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

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

NOTE: Cet équipement a été testé et jugé conforme aux limites pour un dispositif numérique Classe A, conformément à la partie 15 des Règles FCC. Ces limites sont conçues pour fournir une protection valable contre les interférences dangereuses au sein d'une installation professionnelle. Cet équipement génère, utilise et peut émettre une puissance de fréquence radio et, s'il n'est pas installé et utilisé selon les instructions, il peut provoquer des interférences dangereuses aux communications radio. Dans un environnement résidentiel, ce dispositif peut provoquer des interférences ; Dans ce cas l'utilisateur devra remédier à ses frais à ces interférences.

Présentation du MorphoAccess®

Le MorphoAccess® est un terminal de reconnaissance d'empreintes digitales dédié aux applications de contrôle d'accès physique et de contrôle horaire offrant des capacités d'identification multiples avec un niveau de performances inégalé.

Présentation des Interfaces

Interface Homme-Machine

Le MorphoAccess® Série 500 offre une interface homme-machine simple et ergonomique dédiée au contrôle d'accès basé sur la reconnaissance des empreintes digitales :

- un scanner optique dédié à la lecture des empreintes (1),
- une « LED » multi couleurs (2),
- un « buzzer »,
- un lecteur pour lire les empreintes de référence à partir de la carte sans contact (voir chapitre « Objet du document ») (3),
- un clavier pour les fonctions de contrôle horaire, la configuration et le code PIN (4),
- un écran 128 x 64 (5).



Figure 1: Face avant du terminal MorphoAccess® Série 500

Interfaces électriques

Le terminal offre de nombreuses interfaces dédiées aux informations de contrôle et d'administration :

- une sortie Wiegand / Dataclock multiplexée pour exporter l'identifiant de l'utilisateur vers un contrôleur (1),
- une sortie RS422 ou RS485 (2),
- une sortie du type « LED OUT » (3),
- deux d'entrées du type « LED IN » pour une intégration optimale dans un système de contrôle d'accès physique (4),
- un relais pour commander directement un accès (serrure de porte) (5),
- un capteur anti-vandalisme pour détecter une intrusion (6),
- une entrée Wiegand / Dataclock multiplexée pour recevoir l'identifiant de l'utilisateur à partir d'un lecteur de carte externe (7),
- une interface Ethernet (LAN 10/100 Mbps) permettant la gestion à distance par TCP/IP (8),
- une interface Ethernet permettant l'alimentation électrique par câble Ethernet (Power Over Ethernet) (9).

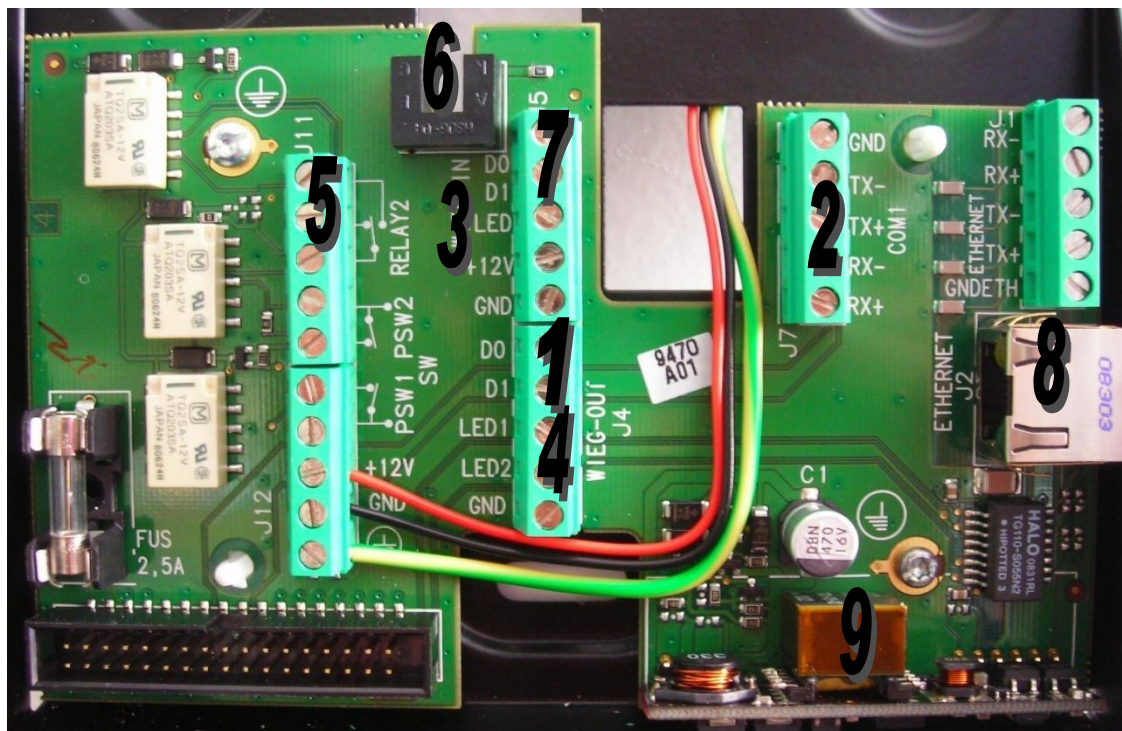


Figure 2: Bornier du terminal MorphoAccess® Série 500

Le Manuel d'Installation décrit les caractéristiques de chaque interface et les procédures de connexion.

Synoptique d'un système de contrôle d'accès physique

Architecture type

L'architecture type comprend un MorphoAccess®, une Station d'Enrôlement et un Contrôleur Central.

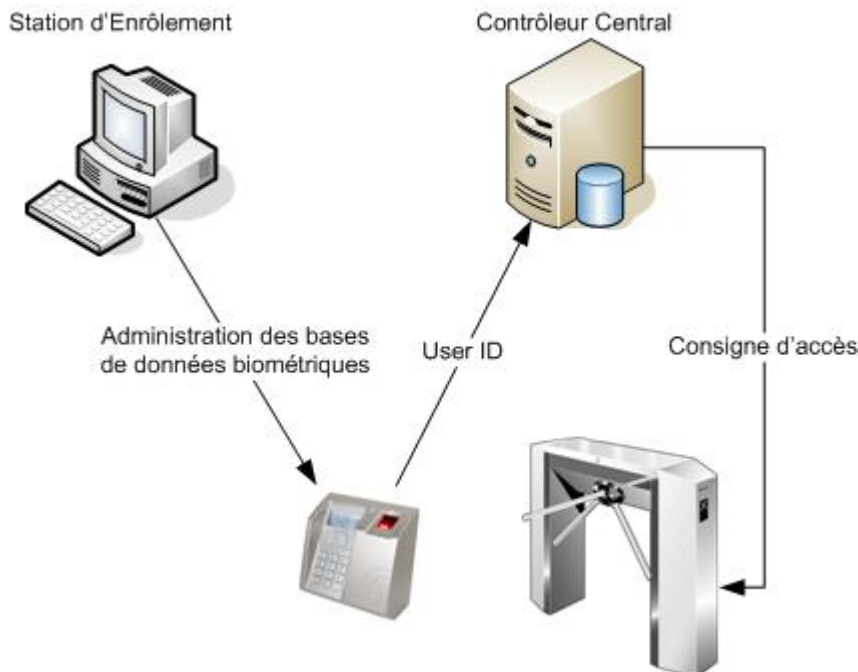


Figure 3: Architecture typique d'un système de contrôle d'accès

Gestion de la base de données biométriques du MorphoAccess®

La gestion de la base de données biométriques interne du MorphoAccess® peut être effectuée soit localement (par l'Interface Homme-Machine du terminal), soit à distance par une Station d'Enrôlement (généralement MEMS™). Ces deux modes de gestion exclusifs sont définis comme le :

- mode de gestion local,
- mode de gestion à distance.

Mode de fonctionnement du MorphoAccess®

Le MorphoAccess® fonctionne selon deux modes exclusifs.

- En *Mode Autonome* (terminal mis en réseau ou pas connecté), le terminal exécute deux types d'applications : *Contrôle d'accès ou Contrôle horaire*. Lorsque le terminal est mis en réseau, la base de données biométriques peut être gérée par une Station d'Enrôlement et téléchargée vers le MorphoAccess®. Lorsque le terminal n'est pas mis en réseau, la base de données est gérée localement.
- Par opposition au *Mode Autonome*, en *Mode « Proxy »* le terminal est commandé à distance par une application hôte qui envoie des commandes unitaires au MorphoAccess®.

Envoi des résultats du MorphoAccess®

Lorsque l'identification biométrique est positive, l'identifiant (ou matricule, ou numéro d'identifiant ou « ID ») de la personne peut être envoyé au Contrôleur Central qui décidera d'autoriser l'accès.

Présentation du terminal

Un MorphoAccess® Série 500 fonctionne avec 4 applications répondant à un besoin spécifique.

Application de Contrôle d'Accès (MACCESS)

Il s'agit de l'application principale dédiée au contrôle biométrique.

Il est possible de quitter cette application pour en lancer d'autres.

Ce *Manuel Utilisateur* détaille les caractéristiques de cette application.

Application d'Enrôlement Local (ENROLMENT)

Cette application permet d'enrôler les utilisateurs dans le terminal lorsque le MorphoAccess® n'est pas connecté à un réseau externe (Mode de gestion locale).

La base de données créée peut être enregistrée chiffrée sur une clé USB et exportée vers un autre MorphoAccess® autonome.

Il est aussi possible de créer des badges MIFARE® et/ou DESFire® contenant les empreintes des utilisateurs (selon le terminal, voir la section « Objet du document »).

Un message de synchronisation peut être envoyé à un hôte distant pour l'informer des changements effectués sur les bases biométriques.

L'accès à cette application est protégé par le mot de passe qui autorise la gestion des utilisateurs (« *User Management Password* »).

Application de configuration (CONFIGURATION)

Cette application permet de modifier les paramètres de l'application principale.

Les paramètres sont organisés en section.

L'accès à cette application est protégé par le mot de passe qui autorise la configuration du terminal (« *Terminal Configuration Password* »).

Lecture des événements de contrôle d'accès (LOGVIEWER)

Cette application permet de consulter le journal d'événement local enregistré par le MorphoAccess®, et de l'exporter sur une clé USB.

L'accès à cette application est protégé par le mot de passe qui autorise la gestion des utilisateurs (« *User Management Password* »).

Synthèse de l'architecture multi-applicative

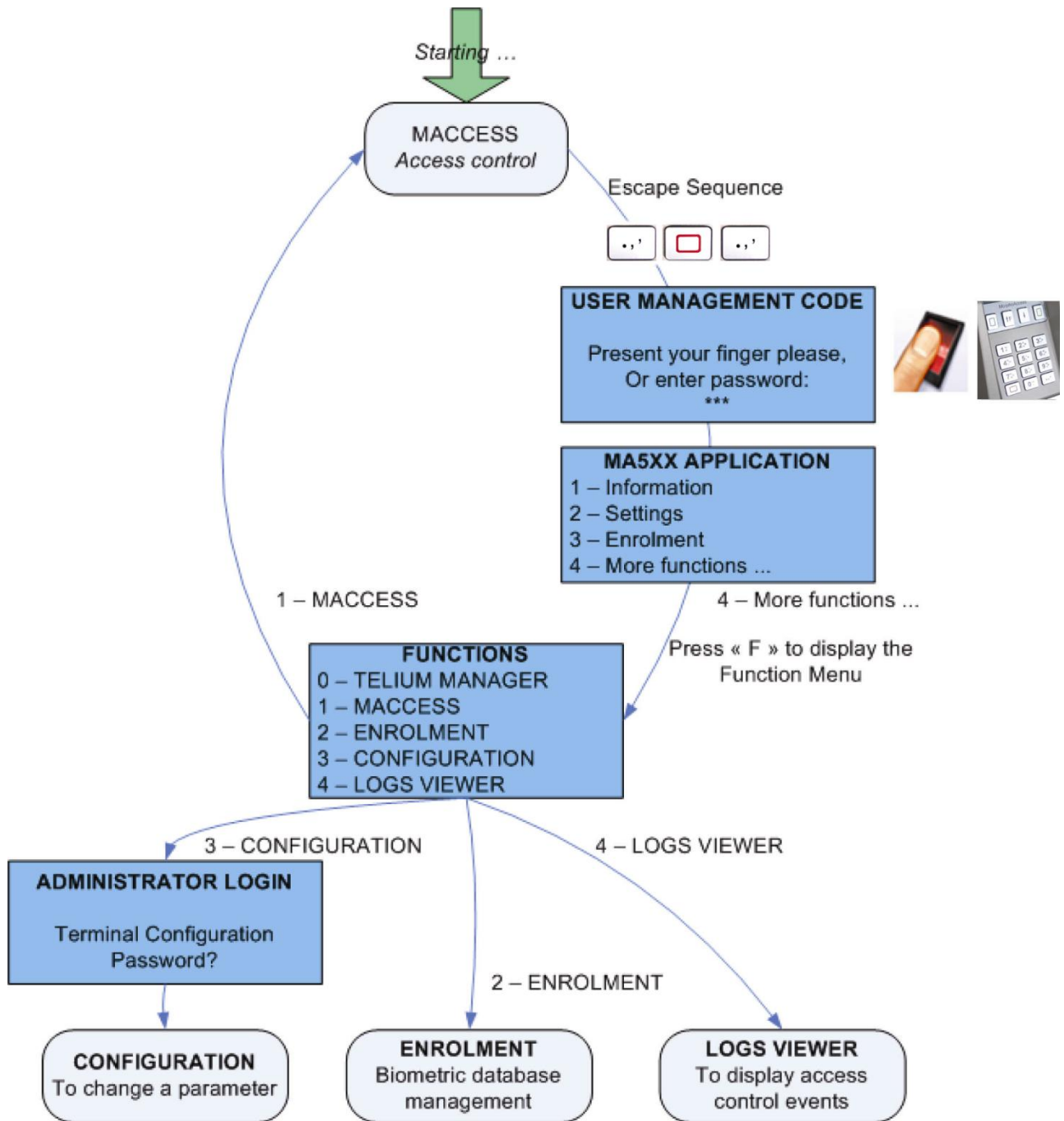


Figure 4: Synthèse des applications du terminal MorphoAccess® Série 500

Présentation du Contrôle d'Accès

Le MorphoAccess® fonctionne selon deux modes de reconnaissance biométrique : identification ou authentification. L'identification et l'authentification peuvent être actives en même temps (mode fusionné ou multi-facteurs).

Identification (1 contre N)

L'empreinte capturée par le MorphoAccess® est comparée dans une base de données – 1 contre N.

Les empreintes biométriques sont enregistrées dans la base de données locale du terminal. Selon la licence installée, le terminal peut stocker 3 000 utilisateurs (2 doigts par utilisateur) dans sa base de données locale ou 50 000 utilisateurs répartis sur 5 bases de 10 000 utilisateurs chacune.

Dans ce mode, le capteur sera toujours allumé, en attente d'un doigt. L'empreinte saisie est comparée avec celles stockées dans la base de données.



Figure 5: Mode Identification

Si l'utilisateur est reconnu, l'ID peut-être renvoyé au Contrôleur Central.

Si l'utilisateur n'est pas reconnu, un message de non-reconnaissance peut-être envoyé au Contrôleur Central.

La section [Contrôle d'accès par Identification](#) détaille plus amplement ce mode de fonctionnement

Authentification avec les empreintes de référence dans la carte (1 contre 1)

L'empreinte capturée par le MorphoAccess® est comparée avec une empreinte de référence – 1 contre 1.

Cette empreinte de référence est lue au préalable sur une carte « sans contact » MIFARE® ou DESFire®.



Figure 6: Mode authentication

Si l'utilisateur est reconnu, l'ID peut-être renvoyé au Contrôleur Central.

Si l'utilisateur n'est pas reconnu, un message de non-reconnaissance peut-être envoyé au Contrôleur Central.

La section [Contrôle d'accès par Authentification](#) détaille plus amplement ce mode de fonctionnement

Authentification avec les empreintes de référence dans le terminal (1 contre 1)

L'empreinte saisie est comparée avec une empreinte de référence – 1 contre 1.

L'empreinte de référence de l'utilisateur est enregistrée dans la base de données locale. Dans ce cas, l'identifiant de l'utilisateur est utilisé en tant que clé pour trouver l'empreinte de référence. L'identifiant de l'utilisateur peut être envoyé par Wiegand, DataClock, saisi sur clavier ou enregistré sur une carte sans contact MIFARE® ou DESFire®.

Reconnaissance fondée sur plusieurs facteurs

Il est possible de combiner plusieurs facteurs d'identification tels que, « ce que j'ai » (une carte à puce sans contact), « ce que je sais » (code PIN) et « ce que je suis » (empreintes biométriques).

Mode proxy

Le *mode proxy* n'est pas un mode de reconnaissance à proprement parler. Dans ce mode, le MorphoAccess® fonctionne en tant qu'esclave attendant des commandes externes telles que :

- identification,
- vérification,
- activation du relais,
- lecture des données sur une carte sans contact,

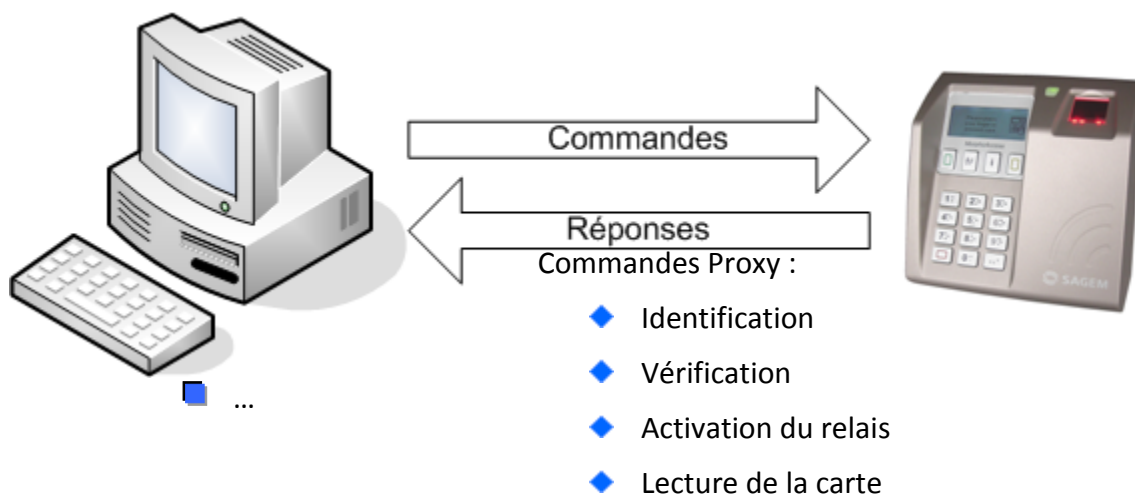


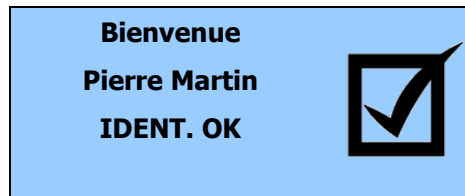
Figure 7: Mode Proxy

Le chapitre [Mode proxy](#) fournit plus d'informations sur la gestion à distance.

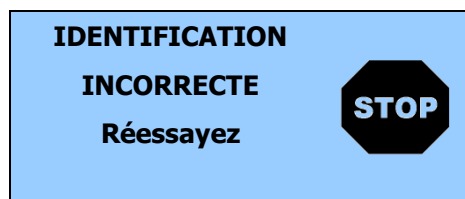
Le document *MorphoAccess® Host System Interface Specification* détaille l'ensemble des commandes relatives à ce mode d'administration.

Envoi de l'ID au Contrôleur central de Sécurité

Si l'utilisateur a été reconnu, le terminal peut déclencher l'accès (activation d'un relais) ou envoyer l'ID de la personne reconnue au Contrôleur Central.



Si l'utilisateur *n'a pas* été reconnu, le terminal peut retourner un message d'erreur au Contrôleur Central.



En plus des informations utilisateur, le terminal peut :

- activer un relais interne (qui peut ouvrir une porte),
- enregistrer le résultat de la demande d'accès dans un fichier journal;
- et envoyer un message de résultat de la demande d'accès à un système à distance (généralement un Contrôleur Central de Sécurité) à travers différents liens de communication.



Résultat du contrôle :

- ◆ RS485 ou RS422
- ◆ Wiegand ou DataClock
- ◆ Ethernet ou Wi-Fi™ (UDP / TCP / SSL)

Figure 8: Envoi du résultat du contrôle de droits d'accès

Le résultat du contrôle d'accès peut être transmis au travers de diverses interfaces.

Relais

Lorsque cette fonction est activée, le relais du MorphoAccess® est activé pendant la période spécifiée en cas de contrôle d'accès réussi (l'accès est autorisé).

Port série Wiegand/ DataClock

Le résultat du contrôle d'accès peut être envoyé en utilisant soit le protocole Wiegand soit le protocole DataClock.

Le format du message inclut uniquement l'ID utilisateur (qui doit être au format numérique). Par défaut, le message est envoyé seulement si le résultat du contrôle d'accès est positif. Cependant, il est possible de définir l'envoi d'un message en cas de résultat négatif contenant un message d'erreur à la place de l'ID de l'utilisateur.

Port Ethernet

Le résultat du contrôle d'accès peut être envoyé via une connexion IP en utilisant soit par le protocole UDP, soit le protocole TCP, soit le protocole SSL.

Le format du message inclut la date/heure du contrôle d'accès, l'ID de l'utilisateur, et le résultat du contrôle d'accès, autorisé ou refusé, ainsi que la raison en cas de refus.

Pour l'IP, l'administrateur peut régler le port et définir le protocole utilisé.

Pour utiliser le protocole SSL, se référer au document *SSL Solution for MorphoAccess®*.

Connexion WI-FI™

A la place d'une connexion Ethernet, il est possible d'utiliser une connexion sans fil. Se référer aux paragraphes [Wizard WI-FI™](#) et [Configuration du mode WI-FI™](#).

Le format du message et les protocoles supportés sont les mêmes : UDP, TCP ou SSL.

Il n'est pas possible de connecter le terminal à travers l'Ethernet et le WI-FI™ en même temps.

WI-FI™ est une marque enregistrée de WI-FI™ Alliance.

Port série RS485/422

Le résultat du contrôle d'accès (au format ASCII) peut être envoyé en utilisant soit le protocole RS485 soit le protocole RS422. Le format du message est identique à celui utilisé pour l'IP.

Lorsque le port série est utilisé pour la gestion du terminal, il n'est pas possible d'envoyer le résultat du contrôle d'accès à travers ce port.

Journalisation du contrôle d'accès

Lorsque cette fonction est activée, le terminal crée une sauvegarde de chaque contrôle d'accès dans un fichier local. Chaque enregistrement inclut :

- la date/heure de contrôle d'accès,
- l'ID de l'utilisateur (si disponible),
- et le résultat du contrôle local des droits d'accès.

Le contenu de ce fichier peut être chargé par la Station d'Enrôlement, affiché sur le terminal ou encore exporté sur une clé USB.

Ce fichier peut contenir jusqu'à 65000 enregistrements : lorsque le fichier est plein, la journalisation du contrôle d'accès s'arrête automatiquement.

Configuration du terminal

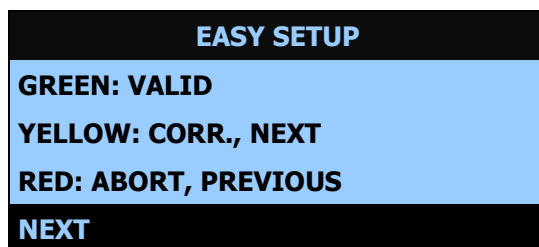
Ce chapitre détaille la manière de configurer le MorphoAccess®. Un paramètre peut être modifié directement sur le terminal ou à distance par réseau.




Un assistant à la configuration appelé « EasySetup » aide l'administrateur à définir rapidement une configuration compatible avec un système de contrôle d'accès existant.

Assistant d'installation (EasySetup)

Initialisation de l'assistant

Lorsque le MorphoAccess® démarre pour la première fois, un « assistant » aide l'administrateur à configurer les principales fonctions.



- La touche  valide le choix.
- La touche  corrige ou passe à l'étape suivante.
- La touche  annule l'opération et retourne à l'étape précédente.

Choix de la langue

Il est possible de choisir la langue de l'application parmi les langues installées.



Configuration de la date et de l'heure

La date et l'heure peuvent être configurées.

Le format de la date est **MM/DD/AAAA (mois/jour/année)**

La touche  efface un caractère.

La touche  valide le choix.

ENTER DATE
08/25/200_
MM/DD/YYYY
VALID

Paramètres du réseau

Configuration dynamique ou statique

Il est possible de faire un choix entre la configuration statique ou dynamique.

DHCP	
1 – Enable	[•]
2 – Disable	[]]

DHCP désactivé

Si le mode DHCP est désactivé, les paramètres suivants, de l'interface Ethernet, doivent être renseignés :

- l'adresse IP,
- masque du réseau,
- passerelle de connexion par défaut.

ENTER IP ADDRESS
10.10.161.3_
VALID

DHCP activé

En DHCP, seul le nom du terminal sur le réseau est nécessaire.



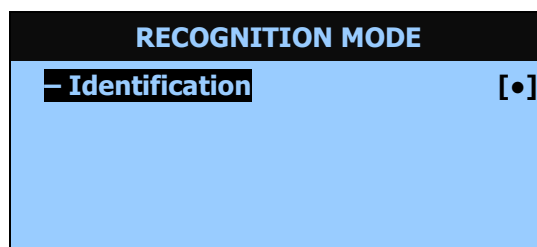
Le serveur DNS doit être mis à jour pour prendre en compte le nom d'hôte du MorphoAccess®. Cela permet aux utilisateurs d'utiliser directement ce nom d'hôte dans les différentes applications. Veuillez contacter votre administrateur réseau.

Mode reconnaissance

Dès que les paramètres réseau sont définis, l'étape suivante consiste à définir le mode reconnaissance.

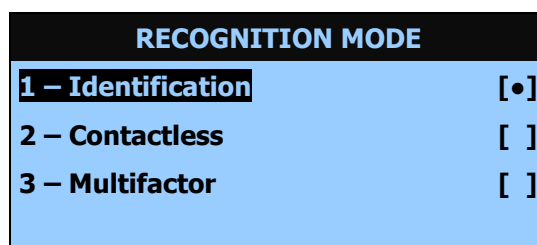
L'écran de sélection du Mode reconnaissance dépend du type de terminal (voir chapitre « Objet du document »).

Sur les MorphoAccess® non-équipés de lecteur de cartes sans contact:



Seul le mode de reconnaissance peut être sélectionné.

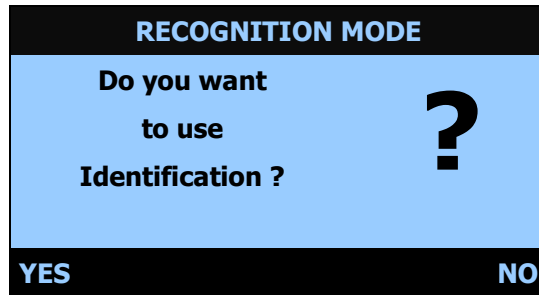
Sur les MorphoAccess® équipés uniquement d'un lecteur de cartes sans contact MIFARE®.



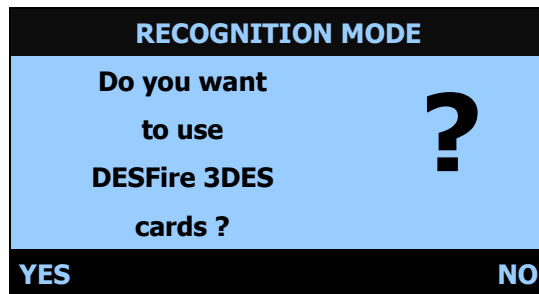
Le terminal peut être configuré soit en mode Identification, soit en mode Authentification Sans Contact soit en mode Fusionné (les modes Identification et Authentification Sans Contact sont actifs simultanément).

Sur les MorphoAccess® équipés d'un lecteur de cartes sans contact MIFARE®/DESFire®:

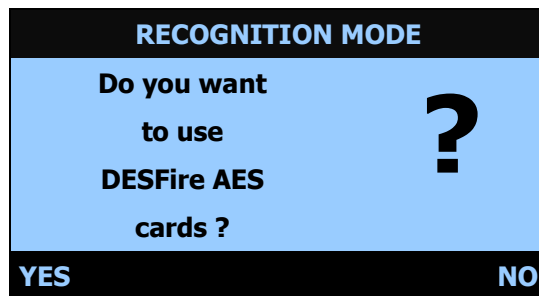
Activer ou non l'Identification:



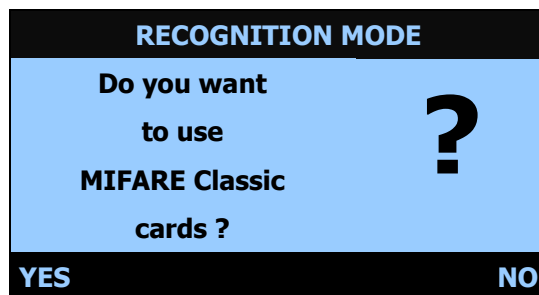
Activer ou non la lecture de cartes DESFire® 3DES :



Activer ou non la lecture de cartes DESFire® AES:



Activer ou non la lecture de cartes MIFARE®:



Par exemple, si l'on répond YES à toutes les questions, le terminal sera en mode Fusionné (Identification + cartes DESFire® 3DES + cartes DESFire® AES + cartes MIFARE®).

Les choix précédents déterminant également les cartes sans contacts supportées lors de l'encodage de l'application d'enrôlement (cf. *MorphoAccess® 500 Series Enrolment Application User Guide*).

Si « Yes » est sélectionné pour la lecture des cartes MIFARE®, le terminal pourra encoder des badges MIFARE®.

Si « Yes » est sélectionné pour la lecture des cartes DESFire® 3DES, le terminal pourra encoder des badges DESFire® 3DES, sauf si « Yes » est sélectionnée pour la lecture des badges DESFire® AES. Dans ce cas, le terminal pourra encoder les badges DESFire® AES mais pas les badges DESFire® 3DES.

Interface de sortie

L'étape suivante permet de définir le protocole utilisé pour communiquer le résultat du contrôle.

INTERFACE PARAMETERS	
1 – Wiegand	[OFF]
2 – DataClock	[OFF]
3 – ID on UDP	[OFF]
4 – Next	

Chaque interface peut être configurée et activée séparément.

Choisir **4 – Next** pour passer à l'étape suivante.

Configuration de Wiegand

Trois protocoles sont disponibles : 26, 34 et 37 bits.

Pour d'autres configurations de Wiegand, référez-vous au chapitre [Authentification - ID lu sur l'entrée Wiegand / DataClock](#).

WIEGAND	
1 – 26 bits	[?]
2 – 34 bits	[]
3 – 37 bits	[]
4 – OFF	[]

Configuration de Dataclock

L'interface Dataclock peut être activée. Elle est cependant multiplexée avec la sortie Wiegand.

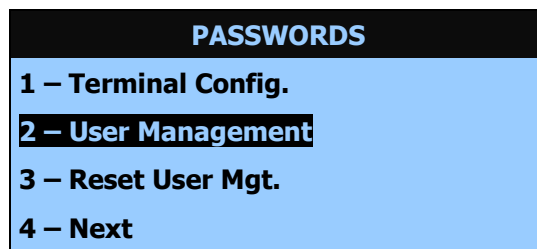
Envoi du résultat par UDP

Le résultat du contrôle peut être émis via Ethernet / WI-FI™ (UDP). L'adresse IP du serveur de destination doit être précisée.

SERVER IP ADDRESS
10.10.161.7_
VALID

Configuration du mot de passe

Cette étape consiste à changer les mots de passe.



Choisir **4 – Next** pour quitter l'assistant.

Le terminal va redémarrer pour appliquer les changements.



Appuyer sur **NEXT** pour redémarrer le terminal.

Appuyer sur **ABORT** pour retourner à la gestion du mot de passe.

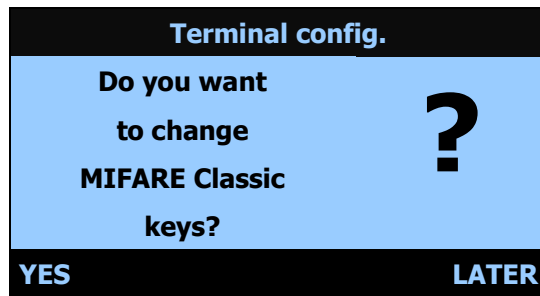
Changement des clés MIFARE®

Ce chapitre concerne uniquement les MorphoAccess® équipés d'un lecteur de cartes sans contact MIFARE® (voir chapitre« Objet du document »).

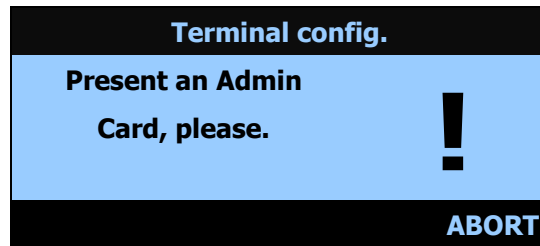
Cette étape est disponible à partir de la version de logiciel embarqué V02.09.

L'assistant propose de remplacer les clés d'usine MIFARE® par les clés utilisateur MIFARE® à l'aide d'un badge administrateur (badge contenant les nouvelles clés MIFARE®).

L'écran suivant est affiché :



Si l'on choisit de changer les clés, l'écran suivant s'affiche et la présentation d'un badge administrateur doit être faite :



Dès que le badge administrateur est détecté, les clés MIFARE® sont automatiquement mises à jour dans le terminal (la progression de la mise à jour est signalée par une succession de bips).

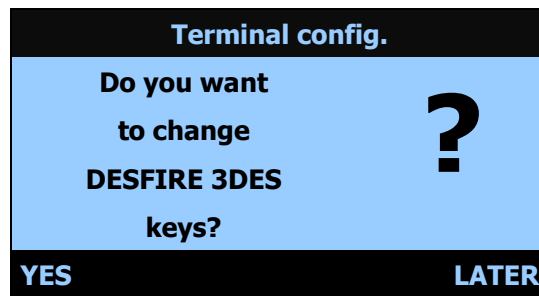
Voir le document *MorphoAccess® 500 Series Enrolment Application User Guide* pour de plus amples informations sur l'encodage du badge administrateur.

Changement des clés DESFire®

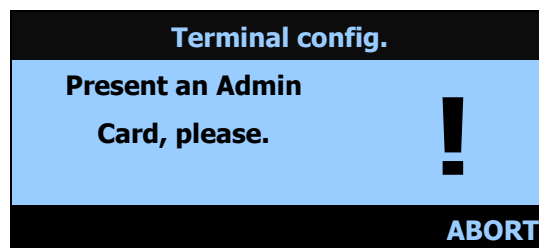
Ce chapitre concerne uniquement les MorphoAccess® équipés d'un lecteur de cartes sans contact DESFire® (voir chapitre «[Objet du document](#) »).

L'assistant propose de remplacer les clés d'usine DESFire® 3DES par les clés utilisateur DESFire® 3DES à l'aide d'un badge administrateur (badge contenant les nouvelles clés DESFire®).

L'écran suivant est affiché :

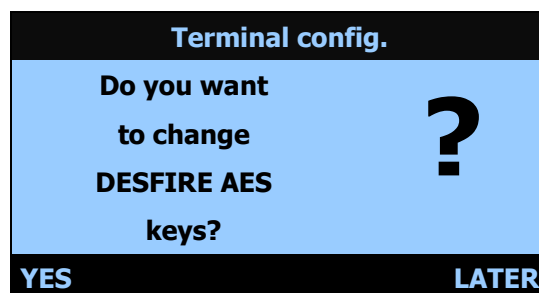


Si l'on choisit de changer les clés, l'écran suivant s'affiche et la présentation d'un badge administrateur doit être faite :



Dès que le badge administrateur est détecté, les clés DESFire® 3DES sont automatiquement mises à jour dans le terminal (la progression de la mise à jour est signalée par une succession de bips).

Un procédé similaire est ensuite proposé pour le changement des clés DESFire® AES :

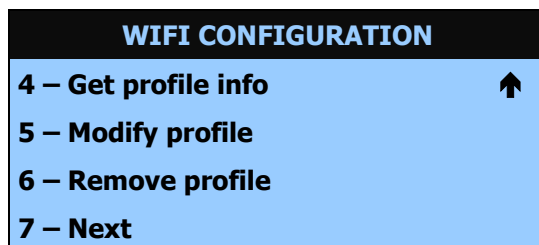
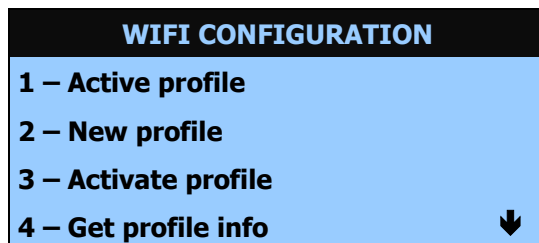


Voir le document *MorphoAccess® 500 Series Enrolment Application User Guide* pour de plus amples informations sur l'encodage du badge administrateur.

Wizard WI-FI™ (à partir de la version 2.09 du logiciel embarqué)

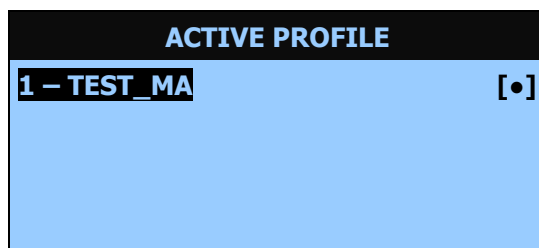
Cette étape consiste à configurer les communications sans fil en mode WI-FI™, si un adaptateur WI-FI™ USB est connecté au MorphoAccess®, et si une licence WI-FI™ est chargée dans le terminal (voir « [Configuration du mode WI-FI™](#) »).

Le Wizard WI-FI™ permet de réaliser les opérations suivantes :



Visualisation du profil actif

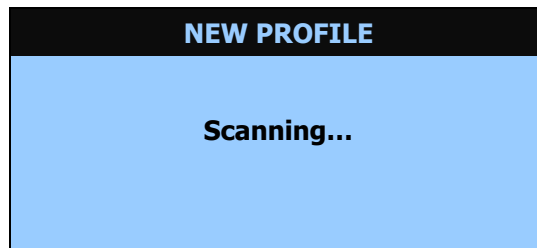
Le choix **1 – Active profile** permet de visualiser le profil actif :



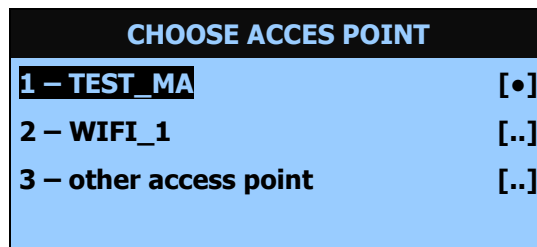
Création et activation d'un profil

Le choix **2 – New profile** permet de créer et d'activer un profil.

Dans une première phase le système commence par rechercher les points d'accès WI-FI™ disponibles. L'écran suivant s'affiche temporairement :

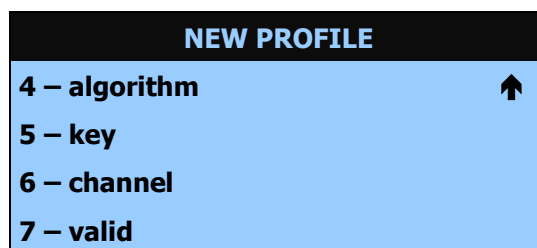
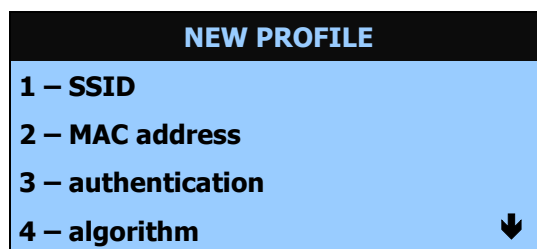


Puis la liste des points d'accès WI-FI™ s'affiche :



Dans une seconde phase, il faut choisir un point d'accès WI-FI™ existant ou un autre point d'accès pour créer le nouveau profil.

Le menu suivant s'affiche et permet de fixer chacun des paramètres du nouveau profil :



Plusieurs paramètres sont automatiquement initialisés durant la première étape – SSID, adresse MAC, chaîne. D'autres paramètres doivent être initialisés par l'administrateur réseau :

- le SSID (Service Set Identifier) est le nom du profil,
- l'adresse MAC est celle du point d'accès,
- le mode d'authentification peut être : « open » ou « shared »,
- l'algorithme peut être : « None », « WEP64 », « WEP128 » ou « WPA-PSK »,

- la clé à saisir est hexadécimale de longueur 10 pour le WEP64, 26 pour le WEP128, ou une chaîne ASCII de 8 à 63 caractères pour le WPA-PSK,
- le canal peut être changé pour éviter des interférences.

Si l'on utilise un point d'accès existant, les paramètres ont initialement les valeurs de ceux du point d'accès ; pour un autre point d'accès, les paramètres ont des valeurs par défaut.

Si un algorithme WEP est choisi, la clé doit être renseignée (elle n'est pas récupérée du point d'accès).



Le profil doit avoir les mêmes paramètres que son point d'accès.

Pour la sélection d'un des six premiers choix, des écrans de saisie ou des menus s'affichent. Le choix **7 – valid** permet de créer et d'activer le profil avec ses paramètres.

Activation d'un profil

Le choix **3 – Activate profile** permet d'activer un profil.

Un écran listant les profils créés au niveau du MorphoAccess® est affiché et permet le choix du profil à activer.

Les paramètres sont activés après le redémarrage du terminal.

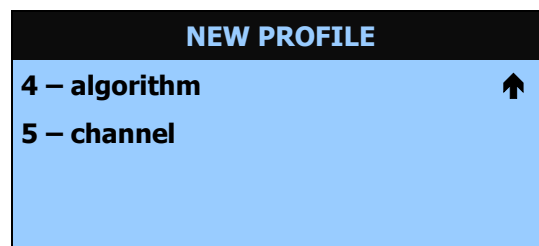
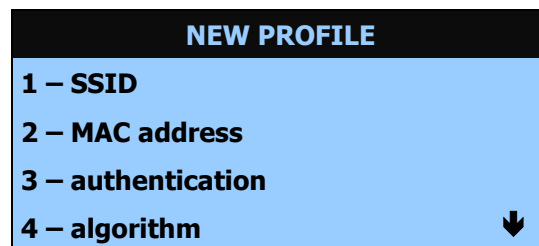
Il est possible de vérifier la bonne configuration WI-FI™ en lisant l'adresse IP affectée au terminal par le réseau WLAN : l'adresse IP doit être différente de 0.0.0.0., si la configuration a été sélectionnée.

Visualisation des informations d'un profil

Le choix **4 – Get profile info** permet de récupérer des informations sur un profil.

Un écran listant les profils existants au niveau du MorphoAccess® est d'abord affiché et permet le choix du profil.

Une fois le profil sélectionné, l'écran suivant s'affiche :



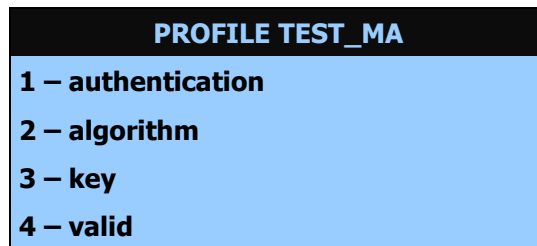
Les différents paramètres peuvent être visualisés.

Modification d'un profil


Le choix **5 – Modify profile** permet de modifier certains paramètres d'un profil.

Un écran listant les profils existants au niveau du MorphoAccess® est d'abord affiché et permet le choix du profil.

Une fois le profil sélectionné, l'écran suivant s'affiche :



Si un algorithme WEP ou WPA est choisi, la clé doit être renseignée (elle n'est pas récupérée).

 Le profil doit avoir les mêmes paramètres que son point d'accès.

Pour la sélection d'un des **trois premiers** choix, des écrans de saisie ou des menus s'affichent. Le choix **4 – valid** permet de modifier et d'activer le profil avec ses paramètres.

Suppression d'un profil

Le choix **6 – Remove** permet de supprimer un profil.

Un écran listant les profils existants au niveau du MorphoAccess® est affiché et permet le choix du profil à supprimer.

Configuration des paramètres réseau du profile actif (depuis la version 2.11 du logiciel embarqué)

Le choix **7 – Next** permet de choisir entre une configuration IP statique ou dynamique (DHCP).

DHCP	
1 – Enable	[•]
2 – Disable	[..]

DHCP désactivé

Si le protocole DHCP n'est pas choisi, les paramètres suivants doivent être renseignés :

- adresse IP,
- Masque de sous-réseau,
- Passerelle par défaut.

DHCP activé

Lorsque le protocole DHCP est choisi, l'assistant demande de saisir le nom d'hôte du terminal.

ENTER HOSTNAME
MA0789652_
VALID

Le serveur DNS doit être mis à jour pour que le terminal soit joignable en utilisant directement son nom d'hôte. Veuillez contacter votre administrateur réseau.

Le terminal doit être redémarré pour que les changements soient pris en compte.

Note 1: Si cette étape n'est jamais effectuée, le terminal configure l'interface WI-FI™ mode dynamique (DHCP).

Note 2: Les paramètres réseau ne sont valides que pour le profile courant.

Rappel du Wizard WI-FI™

Le Wizard WI-FI™ peut être réactivé ultérieurement. Les étapes sont les suivantes :

- quitter l'application principale via la [séquence d'échappement](#),
- sélectionner **Wifi Setup** dans le menu **Settings** (seulement si un adaptateur WI-FI™ USB est connecté au MorphoAccess®).

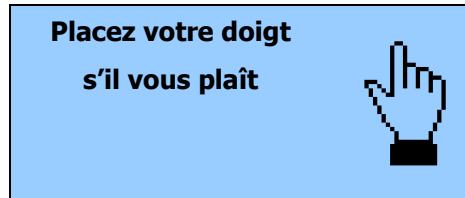
Rappel de l'assistant

L'assistant du MorphoAccess® peut être réactivé ultérieurement. Les étapes sont les suivantes :

- quitter l'application principale via la [séquence d'échappement](#),
- sélectionner **Settings** dans le menu **MA5XX APPLICATION**,
- sélectionner **Easysetup** dans le menu **SETTINGS**.

Menu d'Administration

Accès au Menu Administration

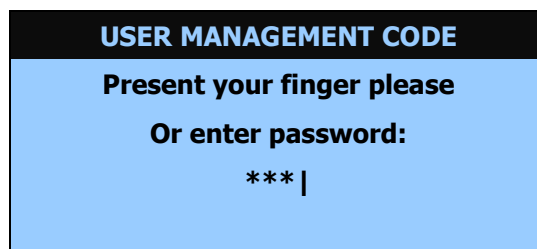


L'application principale peut être interrompue à l'aide d'une séquence de touches (séquence d'échappement). Appuyer sur les touches suivantes l'une après l'autre :

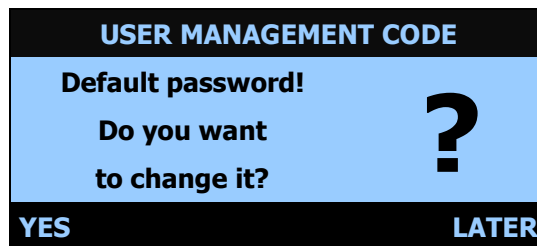


Si la base de données biométriques n'est pas vide, il est possible de substituer la reconnaissance biométrique d'un administrateur à la saisie du mot de passe (« *User Management Password* »).

Par défaut ce mot de passe est « 12345 ».



Si l'Administrateur utilise le mot de passe par défaut, il est recommandé de le changer immédiatement.



Pour des raisons de sécurité, nous vous incitons à changer de mot de passe.

Caractéristiques du Menu Administration

MA5XX APPLICATION
1 – Information
2 – Settings
3 – Enrolment
4 – More functions...

Menu Informations

MA5XX APPLICATION
1 – Information
2 – Settings
3 – Enrolment
4 – More functions...

Choisir **Information** pour avoir accès aux informations du terminal et du capteur :

INFORMATION
1 – Terminal Info
2 – Sensor Info

Informations du terminal

Choisir **Terminal Info** pour avoir accès aux informations suivantes :

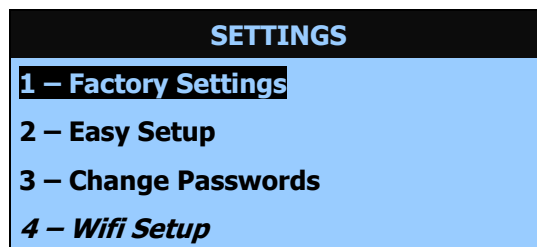
Informations du terminal	Description	Exemple
1 – Type	Type du terminal	520
2 – Serial number	Numéro de série du terminal	073035353A
3 – Version	Version du logiciel principal du terminal (MACCESS)	V02.00.02
4 –IP address	Adresse IP de l'interface utilisée (Ethernet / WiFi)	134.1.32.214
5 –MAC address	Adresse MAC de l'interface utilisée (Ethernet / WiFi)	00:60:4C:69:53:53

Informations du capteur

Choisir **Sensor Info** pour avoir accès aux informations liées au capteur :

Informations du capteur	Description	Exemple
1 – Licence Info	Informations de licence (nom de licence, identifiant de la licence)	MA_XTENDED Device Licence ID: 251946640 0728EC51008
2 – Sensor Info	Informations du capteur (type, taille de la flash, numéro de série, Identifiant du capteur)	MSO300 Flash: 32768 Ko SN: 0730A010026 ID: 25115841-4
3 – Soft. Info	Version du logiciel du capteur. Lors d'une mise à jour un redémarrage du terminal est nécessaire pour voir apparaître la version en cours.	MSO V08.02.d-C

Menu « Settings »



Le choix **Factory Settings** va remettre le terminal en configuration usine. Les paramètres réseaux sont conservés.

Sur les MorphoAccess® équipés d'un lecteur de cartes sans contact MIFARE® (voir chapitre « Objet du document »), il est possible de remettre les clés MIFARE® d'usine.

Sur les MorphoAccess® équipés d'un lecteur de cartes sans contact MIFARE®/DESFire® (voir chapitre « Objet du document »), il est possible de remettre les clés d'usine MIFARE® puis DESFire®.

Le document *MorphoAccess® 500 Series Parameters Guide* donne la valeur usine de chaque paramètre.

Easy Setup permet de relancer « Easy Setup ».

Change Passwords permet de modifier les mots de passe du système.

WiFi Setup permet de configurer l'interface WI-FI™ (seulement si un adaptateur WI-FI™ USB est connecté au MorphoAccess®).

Présentation de la configuration du MorphoAccess®

Présentation

Les paramètres du MorphoAccess® sont enregistrés dans des fichiers organisés en sections.

Par exemple, un fichier intitulé « app.cfg » contient tous les paramètres définissant le fonctionnement de l'application principale.

```
[bio ctrl]
identification=1
nb attempts=2
...
[log file]
enabled=1
...
```

Organisation de la configuration

L'application crée plusieurs fichiers :

- app.cfg,
- adm.cfg,
- bio.cfg,
- net.cfg,
- fac.cfg,
- ...

Veuillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails concernant les fichiers de configuration.

Modification d'un paramètre

Il existe deux possibilités pour changer un paramètre :

- directement sur le terminal à l'aide de l'application de *Configuration*,
- à distance par IP ou par le lien série avec une application client fonctionnant sur la Station d'Enrôlement.

NOTE: Dans ce manuel, un paramètre est présenté à l'aide du formalisme suivant :

« Description rapide du paramètre »	
<i>file/section/parameter</i>	Valeur

Par exemple, pour activer le mode reconnaissance basé sur l'identification, la clé de configuration suivante doit prendre la valeur « 1 » (« enabled », « true » or « yes » lors de l'utilisation de l'application de *Configuration*).

Contrôle d'accès par identification	
<i>app/bio ctrl/identification</i>	1

Modification d'un Paramètre - Application de configuration

L'Application de *Configuration* permet de modifier un paramètre directement sur le terminal.


Vous pouvez quitter une application qui serait en cours pour afficher le menu de *sélection d'application*.

Si l'application principale fonctionne, on doit la quitter à l'aide de la séquence d'échappement :



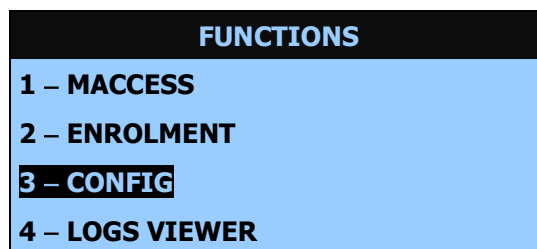
Saisir ensuite le *Mot de passe de la configuration du terminal* pour avoir accès au menu *Administration*.

Sélectionner **More Functions** pour sortir de l'application *Contrôle d'accès*.






Appuyer sur  pour afficher le menu FUNCTIONS.

Choisir **3 – CONFIG** pour lancer l'application de *Configuration*.

Un document spécifique détaille l'*Application de Configuration*. Ce chapitre ne fait que la décrire brièvement.



Rôle des touches

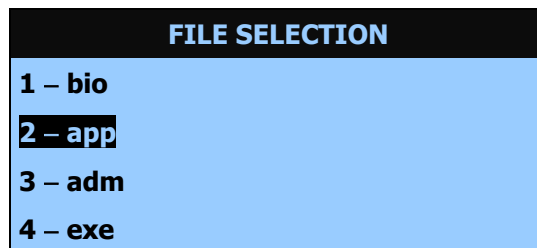
- ➔ Les touches  et  modifient le choix en cours (haut ou bas)
- ➔ La touche  efface un caractère ou retourne à l'écran précédent.
- ➔ La touche  confirme la modification.
- ➔ La touche  quitte l'application.

Modification d'un paramètre

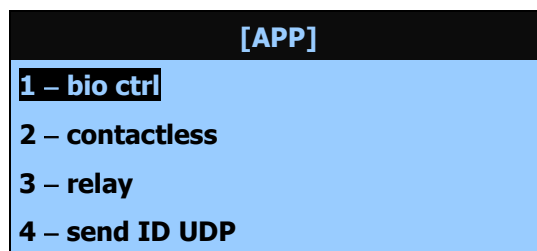
Pour modifier un paramètre, sélectionner "**Configuration...**".



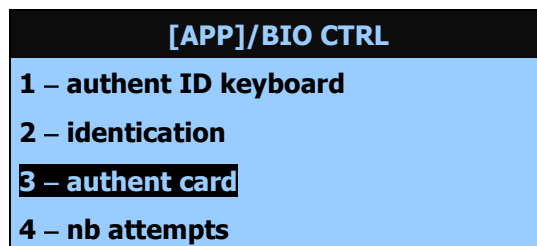
Un menu principal permet de sélectionner le fichier à modifier.



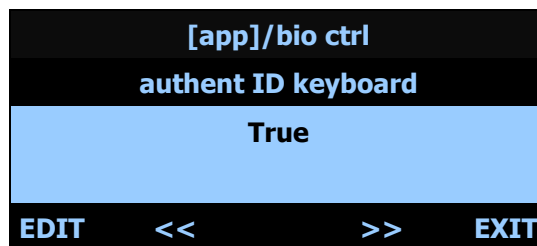
Lorsqu'un fichier a été sélectionné, il est possible de choisir une section de ce fichier.



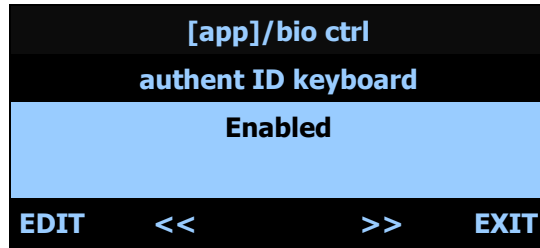
Une liste contient tous les paramètres disponibles dans une section.



Il est possible d'afficher les paramètres un par un dans une section donnée.

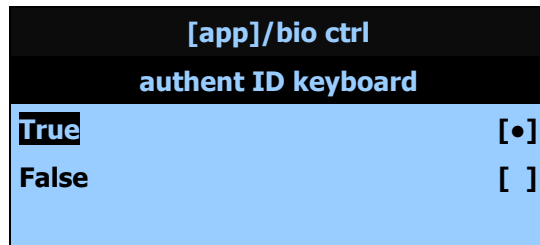


Le menu édition dépendra du type de paramètre.

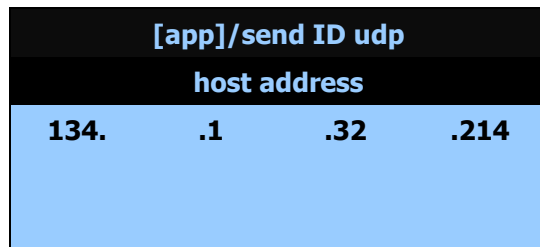


NOTE: Les valeurs "Enabled", "True", "Yes" de l'application de Configuration correspondent à la valeur 1 lors de l'utilisation de l'outil *Morpho Bio Toolbox* par exemple.

Choix binaire



Adresse IP



Configuration d'un MorphoAccess® connecté à un réseau

Introduction

Un PC (fonctionnant avec MEMS™ par exemple) connecté à un MorphoAccess® peut administrer le terminal. Il est possible d'effectuer les actions suivantes :

- ajout d'un enregistrement biométrique,
- modification des paramètres de contrôle,
- lecture de la configuration,
- suppression de la base de données locale,
- suppression d'un enregistrement biométrique,
- récupération du journal des événements,
- mise à jour du logiciel.

Le PC se connecte en tant que client pour le MorphoAccess®.

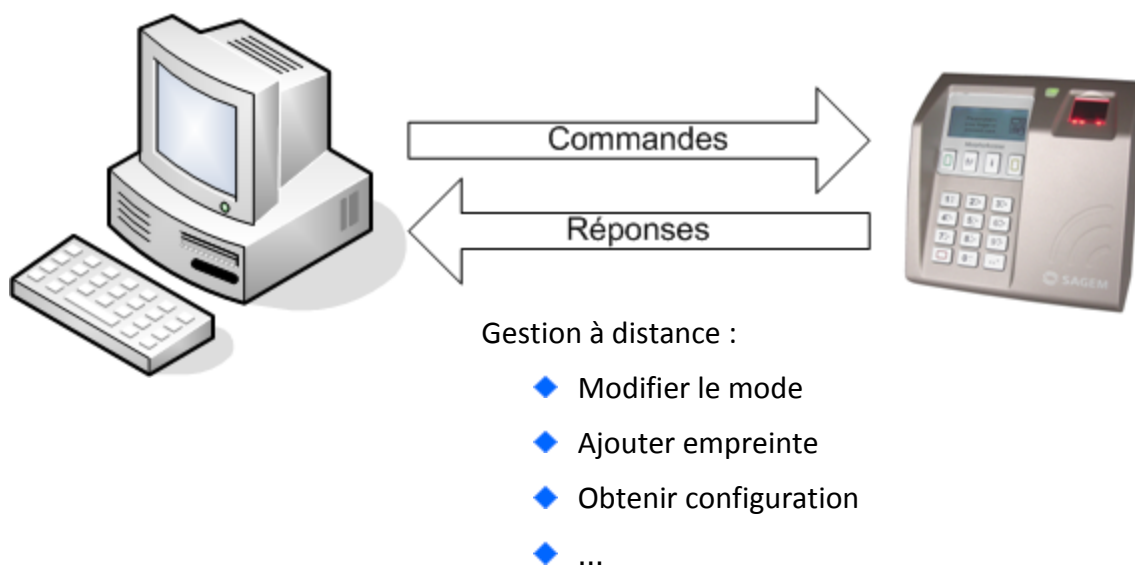


Figure 9: Configuration à distance du terminal MorphoAccess® Série 500

Le MorphoAccess® fonctionne en tant que serveur TCP/IP en attente de la demande provenant d'un PC client.

Le client envoie des enregistrements d'empreintes biométriques au terminal et gère la base de données locale.

Pour une description plus complète de l'administration à distance, veuillez vous référer à la *MorphoAccess® Host System Interface Specification*. Ce document explique comment créer une base de données et stocker des enregistrements d'empreintes biométriques dans cette base.


Paramètres « usine » du réseau

L'adresse IP de l'interface Ethernet du terminal par défaut est *134.1.32.214*. Cette adresse peut être modifiée via IP (*Morpho Bio Toolbox*) ou avec une clé USB (*USB Network Tool*).

Le port du serveur par défaut est 11010.

Paramètres Date/Heure

La date et l'heure du terminal peuvent être initialisées à l'aide de l'assistant de configuration (« Easy setup ») ou d'une application externe telle que l'outil « Morpho Bio Toolbox » (onglet « Configuration » bouton « Régler la date et l'heure ») décrit ci-dessous.

 Le terminal recherche la modification de la date au démarrage et n'accepte pas de différence de plus d'une année. Si la différence dépasse le maximum autorisé, la date est alors réinitialisée à sa valeur précédente. S'il est vraiment nécessaire de modifier la date de plus d'une année, il est possible de le faire en plusieurs étapes de moins d'un an, en redémarrant le terminal entre chaque étape.

Sécurisation en SSL (à partir de la version de logiciel embarqué V02.07)

La communication sur IP peut être sécurisée en SSL. Référez-vous à la documentation *Solution SSL pour MorphoAccess®* pour de plus amples informations.

Modification d'un paramètre à l'aide de l'outil « Morpho Bio Toolbox »

L'outil *Morpho Bio Toolbox* permet de changer des paramètres. Ce programme est une illustration des possibilités d'administration à distance d'un MorphoAccess®. Le Guide d'utilisation est disponible dans le menu « Aide » de l'application *Morpho Bio Toolbox*.

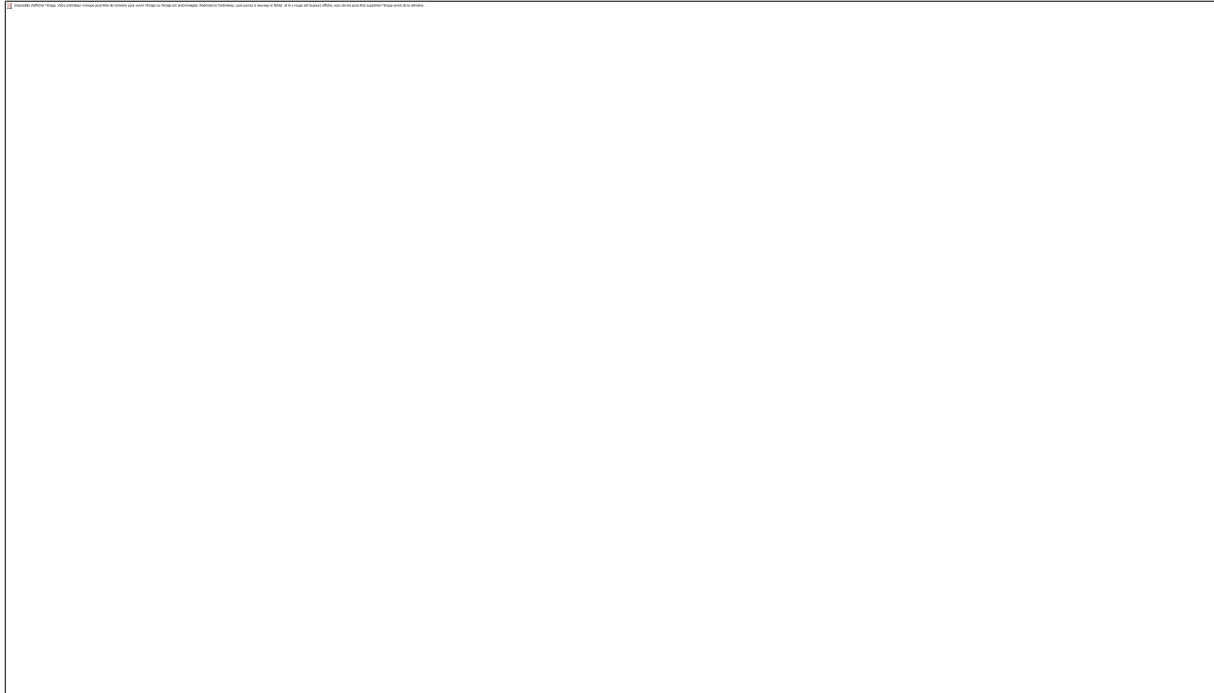


Figure 10: Outil de configuration d'un terminal MorphoAccess®

Configuration du mode WI-FI™ (à partir de la version de logiciel embarqué V02.09)

Le mode WI-FI™ est actif sous les conditions suivantes :

- utilisation d'un adaptateur WI-FI™ USB Morpho, réf. 189930722. La procédure d'installation est décrite dans le *Manuel d'Installation MorphoAccess® Série 500*.
- une licence MorphoAccess WI-FI™ est chargée dans le terminal (cf. Paragraphe [« Téléchargement d'une licence »](#))
- configuration en DHCP de chacun des MorphoAccess® (avec l'outil *Morpho Bio Toolbox* ou *l'EasySetup*).
- pas de connexion Ethernet filaire : le WI-FI™ (WLAN) et l'Ethernet (LAN) sont exclusifs.

Remarque 1 : La présence d'un serveur DHCP et d'un serveur DNS est obligatoire lorsque l'interface WI-FI™ est configurée en mode dynamique (DHCP).

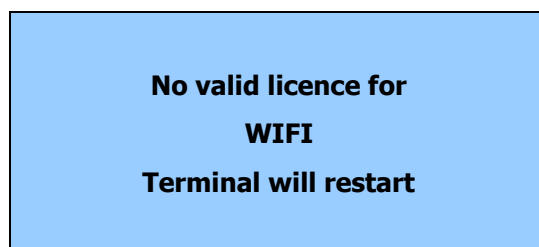
Le serveur DHCP attribue automatiquement une adresse IP à un MorphoAccess®.

Le serveur DNS fait le lien entre le "hostname" du MorphoAccess® et son adresse IP réelle.

Il est aussi important que le serveur DNS soit mis à jour à chaque fois que le serveur DHCP attribue une autre adresse IP à un MorphoAccess®.

Remarque 2 : La présence de la licence WI-FI™ est obligatoire.

Si le terminal est configuré pour utiliser la connexion WI-FI™ avec un adaptateur WI-FI™ USB connecté et sans licence présente, l'écran suivant sera affiché avant que le terminal ne redémarre :



Pour arrêter ces redémarrages, veuillez déconnecter l'adaptateur WI-FI™ et redémarrer le terminal et télécharger une licence.

La description des paramètres WI-FI™ est faite au paragraphe « [Wizard WI-FI™](#) ».

Téléchargement d'une licence

Par défaut, la base de données biométriques du MorphoAccess® peut contenir 3000 utilisateurs. Cette configuration correspond à la licence de base (*MA_3K_USERS*).

La licence MA-Xtended (*MA_XTENDED*) permet d'étendre les capacités de reconnaissance du MorphoAccess® à 5 bases de données de 10000 utilisateurs (2 doigts par utilisateur) ou 16 bases de 3000 utilisateurs.

L'utilisation d'un réseau WI-FI™ (WLAN) est conditionnée par la présence d'une autre licence.

Le numéro de licence dépend du *Device Licence ID*. Cet identifiant peut être récupéré par l'outil de chargement de licence ou afficher via le menu « [Informations](#) ».

L'outil *Terminal Licence Manager* permet de charger l'identifiant de licence dans le MorphoAccess®.

Le document *Terminal License Management User Guide* détaille le processus de chargement d'une licence.

Note : La licence *MA_3K_USERS* correspond à l'ancienne licence *MSO_MA_IDENTLITE*. La licence *MA_XTENDED* correspond à l'ancienne licence *MSO_MA_IDENTPLUS*.

Note : Depuis la version 2.12 du logiciel embarqué, les terminaux de la game MorphoAccess® Série 500 gèrent les licences *MA_3K_USERS* et *MA_XTENDED*, mais aussi les licences *MSO_MA_IDENTLITE* et *MSO_MA_IDENTPLUS* pour compatibilité.

Mise à jour du logiciel embarqué

Il est possible de mettre à jour le logiciel embarqué du MorphoAccess® via IP.





Le répertoire « firmware » du CDROM d'installation contient les outils nécessaires.

L'outil « *MA Quickloader* » est dédié à la mise à jour du système du terminal.

Les procédures de mise à jour sont décrites dans le document *MorphoAccess® Upgrade Tools User Guide*.

Réglage du contraste

Un raccourci clavier permet de régler le contraste de l'écran.

- Les touches  et  augmentent le contraste de l'écran.
- Les touches  et  diminuent le contraste de l'écran.

Application de démarrage

Par défaut, le terminal MorphoAccess® Série 500 démarre avec l'application de contrôle d'accès (MACCESS). Il est possible de définir une autre application de démarrage.

Application de démarrage	
<code>exe/init state/startup</code>	1
	(MACCESS application)

Les choix suivants sont possibles :

- Démarrer sur l'application MACCESS
- Démarrer sur l'application d'enrôlement (ENROLMENT)
- Démarrer sur la liste des applications (écran "Press F to continue").

Veillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails.

Modes autonomes (en Réseau ou déconnecté)

Le MorphoAccess® fonctionne selon deux modes principaux de reconnaissance biométrique : identification ou authentification. L'identification et l'authentification peuvent être activées en même temps, on parle alors de mode fusionné ou multi-facteurs

Au Mode autonome, le terminal peut commander deux applications : Contrôle d'accès ou Contrôle horaire (pointeuse).

Préliminaire : ajout d'une empreinte biométrique dans la base

La gestion de la base de données biométriques interne du MorphoAccess® peut être effectuée soit localement (via l'application d'enrôlement local), soit à distance par une station d'enrôlement. Ces deux modes de gestion exclusifs sont définis comme les :

- mode de gestion local,
- mode de gestion à distance.

Enrôlement en local



L'application d'enrôlement local (*Enrolment Application*) permet d'enrôler des utilisateurs en utilisant directement le capteur du terminal.

Il s'agit d'une application distincte détaillée dans le document *Enrolment Application User Guide*.

La base de données locale peut être exportée chiffrée vers d'autres MorphoAccess® Série 500 à l'aide d'une clé USB.

Il est aussi possible d'encoder des badges contenant les données des utilisateurs (empreintes, noms, ...).

Un message peut être envoyé à un hôte distant pour l'informer que des changements ont été effectués sur la base biométrique du terminal. Puis l'hôte peut demander ces modifications afin de les intégrer dans une base de données centralisée (cf. [Enrôlement sur terminal avec synchronisation](#)).

Veillez vous référer au document *Enrolment Application User Guide* pour une description complète des fonctionnalités.

Gestion de la base d’empreinte à distance

L'utilisateur est enregistré sur une Station d'enrôlement (par exemple un PC possédant MEMS™) et des empreintes biométriques sont exportées vers le MorphoAccess® via IP ou une clé USB.

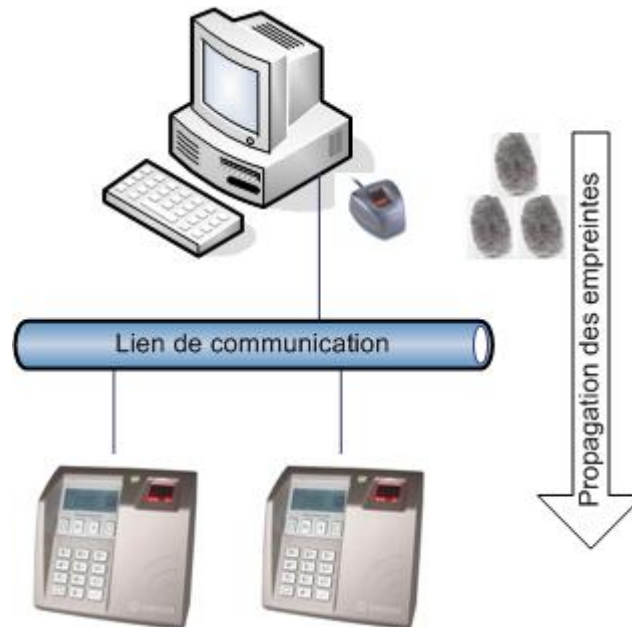


Figure 11: Gestion de base à distance

Cette architecture permet de gérer les bases de données d'un parc de MorphoAccess® à partir d'un PC.

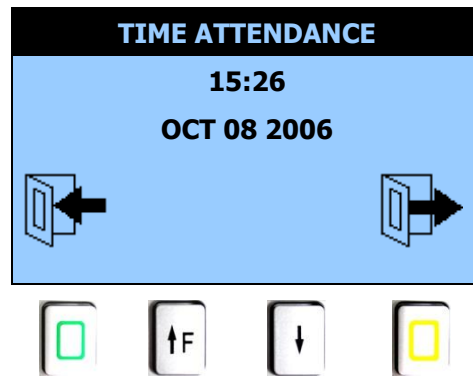
Contrôle d'Accès ou de Pointage

L'application MorphoAccess® peut être configurée pour fonctionner en mode de contrôle d'accès physique ou en mode contrôle horaire (pointage). Dans cette dernière configuration, les événements enregistrés par le MorphoAccess® sont alors enrichis d'informations de pointage (entrée, sortie...).

Lorsque le mode de pointage est activé, l'écran principal peut afficher 2 ou 4 fonctions ou une image.

Mode deux fonctions :

Pointage (2 fonctions)	
<i>app/modes/time and attendance</i>	1



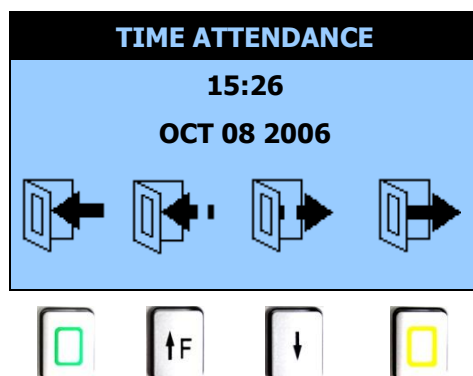
- Touche  : Sélection ENTREE
- Touche  : Sélection SORTIE





Mode quatre fonctions :



Pointage (4 fonctions)

app/modes/time and attendance

2



- Touche  : Sélection ENTREE
- Touche  : Sélection retour d'une absence temporaire
- Touche  : Sélection sortie pour une absence temporaire
- Touche  : Sélection SORTIE

- A son entrée, l'utilisateur doit appuyer sur la touche  pour enregistrer son heure d'entrée.
- A sa sortie, l'utilisateur doit appuyer sur la touche  pour enregistrer son heure de sortie.

Pour des utilisations particulières telles que des absences temporaires, deux fonctions supplémentaires correspondant aux touches de fonction 2 et 3 peuvent être affichées.

Mode étendu:

Pointage (image)

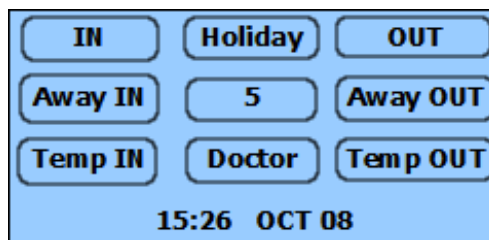
app/modes/time and attendance

3

Dans ce mode chaque touche numérique du clavier peut être associée à une fonction de pointage et une image au format bitmap (qui décrit la correspondance entre le clavier et les fonctions) est affichée à l'écran. Un texte spécifique peut être affiché à l'écran après avoir appuyé sur la touche définie. (Voir *MorphoAccess® Series Parameters Guide* pour plus de détails).

Pour charger une image dans le MorphoAccess® utiliser l'exécutable **BMP2REQ_Generator.exe** et l'outil MATM pour charger le fichier REQ ainsi généré. L'image bitmap doit être encodée en monochrome uniquement et de taille inférieure ou égale à 128 x 50 pixels.


L'écran suivant est l'écran par défaut pré-chargé et constitue un exemple de ce qui peut être fait :



Dans cet exemple, la sélection IN est associée à la touche '1', la sélection OUT à la touche '3', la sélection retour d'une absence temporaire à la touche '7', la sélection d'une absence temporaire à la touche '9'; la touche '5' est associée à la fonction « fonction utilisateur ».

Après la sélection, le MorphoAccess® passe en mode biométrique (identification ou authentification).

La fonction sélectionnée peut être inscrite dans le fichier journal et envoyée au contrôleur d'accès. Dans le mode étendu, le code de la touche est aussi inscrit dans le fichier journal et est envoyé.

En cas de mauvaise manipulation, l'utilisateur peut appuyer sur la touche  pour abandonner l'opération biométrique en cours. Dans ce cas, rien n'est enregistré ou envoyé au contrôleur.

Après 20 secondes d'inactivité en mode biométrique, le terminal retourne à l'écran de sélection. Dans ce cas, le résultat de l'opération est enregistré et/ou envoyé au contrôleur (délai écoulé).

Pour désactiver le mode *Time Attendance* la clé de configuration *app/modes/time and attendance* doit être mise à la valeur 0.

NOTE: D'autres icônes peuvent être choisies pour le mode de pointage horaire. En effet, les icônes des MorphoAccess® Séries 200 et 300 peuvent être utilisées à la place des nouvelles.

Remarque sur l'écart de l'horloge du terminal

L'horloge du terminal a une dérive de +/- 4 s par jour à +25°C. A 50°C, cette dérive peut atteindre -8 s par jour.

Pour assurer une bonne précision horaire, l'horloge du MorphoAccess® doit être synchronisée régulièrement avec une horloge externe.

Contrôle d'accès par identification

Contrôle d'accès par identification

app/bio ctrl/identification

1

Pour configurer le MorphoAccess® dans ce mode, réglez le paramètre *app/bio ctrl/identification* à 1.

Dans ce mode le capteur est allumé en attente de présentation d'un doigt.

**Placez votre doigt
pour identification
s'il vous plaît**



L'utilisateur peut présenter un doigt pour lancer le processus d'identification.

**Retirez votre doigt
Analyse
en cours ...**



Si l'identification est réussie, le terminal déclenche l'accès ou envoie l'ID correspondant au Contrôleur Central.

L'ID peut être envoyé en utilisant différents protocoles. Le document *MorphoAccess® Remote Messages Specification* détaille comment envoyer le résultat du contrôle d'accès vers un contrôleur distant.

Le résultat s'affiche sur l'écran du terminal.

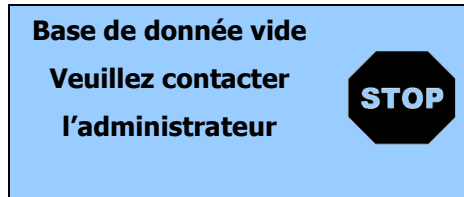
**Bienvenue
Pierre Martin
Ident. OK**



Une fois l'identification de l'utilisateur effectuée, le terminal attend la présentation d'un nouveau doigt.

Un utilisateur au moins (empreinte biométrique) doit être enregistré dans la base de données locale. Via l'enrôlement local, on peut enregistrer jusqu'à 3 000 utilisateurs avec 2 empreintes biométriques chacun.

Si le terminal fonctionne en mode identification avec une base de données vide, le capteur est éteint et l'écran suivant s'affiche.



Désactivation de l'identification

Régler *app/bio ctrl/identification* sur 0 pour désactiver l'identification (Mode proxy).

Contrôle d'accès par identification (licence MA-Xtended)

Il est possible d'augmenter la taille de la base de données biométriques du MorphoAccess® Série 500 par le biais d'une licence (*licence MA-Xtended*) : le MorphoAccess® gère alors 5 bases de 10 000 personnes ou 16 bases de 3000 personnes de façon indifférente.

Contrôle d'accès par identification avec la licence MA-Xtended

app/bio ctrl/identification

1

Pour configurer le MorphoAccess® dans ce mode, réglez le paramètre *app/bio ctrl/identification* sur 1 et vérifiez que la licence *MA-Xtended* a été chargée.

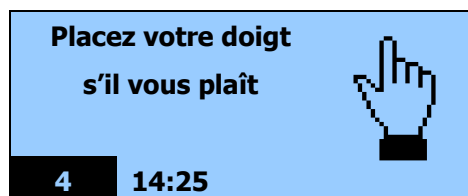
Pour savoir comment mettre à jour le MorphoAccess® avec la licence *MA-Xtended*, veuillez vous référer au chapitre [Téléchargement d'une licence](#).

Si une licence *MA-Xtended* est chargée, il est possible de choisir la base de données active.

Pour choisir une base de données, appuyez simplement sur une touche numérique pour basculer de numéro de base de données.

Par défaut, des bases de données de 0 à 4 peuvent être sélectionnées et utilisées.

La base de données 0 est celle par défaut.



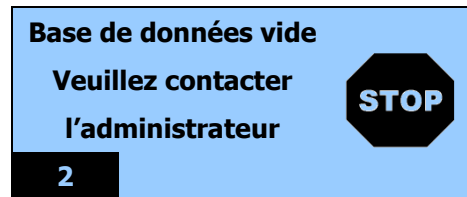
L'utilisateur peut présenter un doigt pour lancer le processus d'identification.

Si l'identification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

Une fois l'identification de l'utilisateur effectuée, le terminal attend la présentation d'un nouveau doigt et sélectionne la base 0.

Une empreinte au moins doit être enregistrée dans la base de données locale.

Si la base de données est vide ou n'existe pas, le capteur est éteint et l'écran suivant s'affiche.




Régler *app/bio ctrl/identification* sur 0 pour désactiver l'identification (Mode proxy).


Sélection de la base de données



La licence *MA-Xtended* étend la capacité de stockage d'empreintes de 1 base de 3 000 utilisateurs à 5 bases de 10 000 utilisateurs. Dans cette configuration, l'utilisateur doit choisir un numéro de base de données (de 0 à 4) avant la présentation d'un doigt pour lancer le processus d'identification.

Pour le confort des utilisateurs du MorphoAccess® Série 300, il est également possible d'activer un mode « 16 bases de données ». Dans ce mode, l'utilisateur sélectionne un numéro de base de données entre 0 et 15 et présente un doigt pour lancer le processus d'identification.

Pour les bases de 0 à 9 appuyez simplement sur un chiffre pour basculer de numéro de base de données.

Pour sélectionner la base de données 3, appuyez sur .

La touche  permet de sélectionner une base de données allant de 10 à 15.

Pour sélectionner la base de données 13, appuyez sur  puis sur .

Les numéros de base valides vont de 00 à 15. Si le numéro de base est supérieur à « 15 », le numéro de la base par défaut (00) est automatiquement forcé.

Compatibilité avec le MorphoAccess® 300	
<i>app/G.U.I./database conversion</i>	500 : mode par défaut – 5 bases 300 : mode 16 bases

Remarque sur le mode « 16 bases »

Du point de vue du terminal, il y a toujours 5 bases de données biométriques.

MorphoAccess® Série 300 ou MorphoAccess® Série 500	MorphoAccess® Série 500 (licence MA-Xtended)
Base de données	Base de données
0,1,2	0
3,4,5	1
6,7,8	2
9,10,11	3
12,13,14,15	4

MEMS™ associe automatiquement l'utilisateur à la bonne base. Par exemple, un utilisateur enregistré dans la base de données 4 sur un MorphoAccess® Série 300 sera enregistré dans la base de données 1 sur un MorphoAccess® Série 500.

Présentation du mode authentification sans contact

Activation du mode lecture de carte sans contact

Sur les terminaux 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

Ces terminaux sont capables 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).

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.

Modes de reconnaissance

De nombreux modes de reconnaissance peuvent être appliqués selon l'emplacement des empreintes (base de données du terminal ou de la carte) et le niveau de sécurité requis.

Le mode de reconnaissance des cartes DESFire® suppose que l'utilisateur approche devant le terminal une carte DESFire® (selon la configuration) contenant des données structurées (identifiant, empreintes biométriques, code PIN,...).

Le mode de reconnaissance des cartes MIFARE® suppose que l'utilisateur approche devant le terminal une carte MIFARE® contenant des données structurées (identifiant, empreintes biométriques, code PIN,...).

Les données sont situées sur la carte par un bloc (paramètre « B ») et sont protégées par une clé (définies par le paramètre « C »). Le paramètre « C » définit la clé à utiliser pendant l'authentification avec la carte.

Pour une description complète de la structure de la carte et du mode d'accès, veuillez vous référer au document *MorphoAccess® Contactless Card Specification*.

Premier bloc à lire	
app/contactless/B	1-215
Numéro de clé à présenter	
app/contactless/C	1, 2, 3

Les modes de reconnaissance suivants sont disponibles :

Authentification avec empreintes biométriques de référence sur la carte

Les empreintes capturées sont comparées avec les empreintes de référence lues sur la carte (PK). L'**identifiant** et les **empreintes biométriques** doivent être enregistrés sur la carte.

Dans ce mode, il est également possible de vérifier un code **PIN** avant l'authentification et de remplacer l'authentification biométrique par une vérification du code **BIOPIN**. Le code BIOPIN est utilisé lorsque les empreintes biométriques de l'utilisateur ne sont pas disponibles (un visiteur par exemple).

Authentification avec empreintes de référence biométriques dans la base de données locale

Les empreintes saisies sont reconnues parmi les empreintes de référence lues dans la base de données locale. Seul l'**identifiant** est nécessaire sur la carte.

Mode d'authentification imposé par la carte

Un tag spécifique, stocké sur la carte définit le déroulement du contrôle (**mode imposé par la carte**).

Il est possible de vérifier le code **PIN** avant l'authentification et de remplacer l'authentification biométrique par une vérification du **BIOPIN**.

Il est également possible de désactiver le contrôle biométrique : dans ce cas, le terminal agit comme un lecteur de carte sans contact contenant seulement un identifiant.

L'authentification sans contact peut être combinée à l'identification locale (mode fusionné, ou encore mode multi-facteurs).

Authentification - empreintes biométriques sur la carte

Authentification - empreintes biométriques dans la carte sans contact

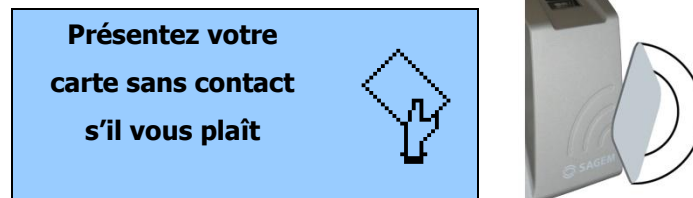
`app/bio ctrl/authent PK contactless`

1

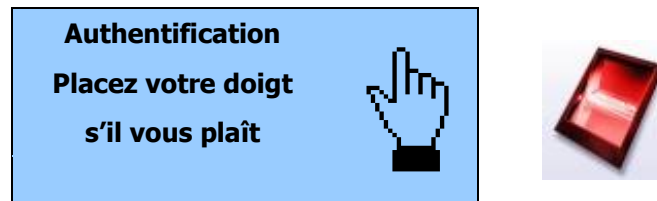
Les MorphoAccess® équipés d'un lecteur de cartes sans contact (voir chapitre « Objet du document ») peuvent fonctionner en *mode authentification sans contact* : l'utilisateur présente sa carte, le terminal lit les empreintes biométriques de référence sur la carte et initie un contrôle biométrique.

Dans ce cas, la carte contient l'identifiant de l'utilisateur et les empreintes biométriques : aucune base de données locale n'est requise.

Pour déclencher l'authentification, l'utilisateur doit présenter sa carte devant le terminal.



Si la carte contient les empreintes de l'utilisateur, celui-ci est invité à présenter son doigt pour l'authentification biométrique.



Si l'authentification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

Une fois l'authentification de l'utilisateur terminée, le terminal attend la présentation d'une nouvelle carte.

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentification sans contact	Oui	Non	Oui	Oui	Non	Non

La structure de la carte est détaillée dans le document *MorphoAccess® Contactless Card Specification*.

Vérification du code PIN – PIN enregistré sur la carte

Si un code PIN de référence est enregistré sur la carte, il est possible de vérifier ce code avant de contrôler les empreintes.

Vérification du code PIN

app/bio ctrl/control PIN

1

Pour déclencher l'authentification, l'utilisateur doit présenter sa carte devant le terminal.

**Présentez votre
carte sans contact
s'il vous plaît**



Si la carte contient un code PIN, l'utilisateur est invité à saisir son code PIN.

**Veillez saisir votre
code PIN**

VAL

COR



S'il s'agit du bon code PIN, l'utilisateur est invité à présenter son doigt pour l'authentification biométrique.

**Authentification
Placez votre doigt
s'il vous plaît**



Si l'authentification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

Il est également possible d'activer ce mode séparément de l'authentification biométrique. Dans ce cas, seul le code PIN est vérifié.

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Vérification du code PIN	Oui	Non	Non	Non	Oui	Non
Authentification et code PIN	Oui	Non	Oui	Oui	Oui	Non

Vérification du code BIOPIN- BIOPIN enregistre sur la carte

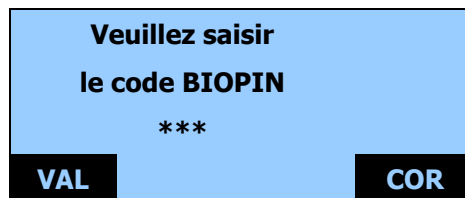
Dans ce mode, la carte doit contenir un code BIOPIN. Le but de ce code est de remplacer l'authentification des empreintes par la vérification d'un code.

Vérification du code BIOPIN	
<code>app/bio ctrl/control BIOPIN</code>	1

Ce mode doit être activé avec l'authentification des empreintes sur la carte (clé de configuration « *authent PK sans contact* » sur 1) Le terminal contrôle si les empreintes sont enregistrées sur la carte. En l'absence d'empreintes, il va alors contrôler le code BIOPIN.

Pour déclencher la vérification du code BIOPIN, l'utilisateur doit présenter sa carte devant le terminal.

Si la carte contient le code BIOPIN de l'utilisateur, celui-ci est invité à le saisir.



S'il s'agit du bon BIOPIN, le terminal déclenche l'accès ou renvoie l'ID de l'utilisateur au Contrôleur Central.

Le contrôle du BIOPIN remplace l'authentification de l'empreinte.

Ce mode peut être combiné à une première vérification du code PIN.

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Vérification du code BIOPIN	Oui	Non	Non	Non	Non	Oui

Authentification - empreintes dans la base de données locale

Dans ce mode, seul l'ID est lu sur la carte. Si l'ID existe dans la base de données biométriques, le MorphoAccess® effectue une authentification à l'aide des empreintes de référence associées à cet ID.

L'ID peut être enregistré dans une structure TLV (généralement une carte encodée par MEMS™) ou directement lu sur un décalage donné de la carte (ID binaire).

ID codé en ASCII, données structurées

Authentification sans contact - empreintes dans la base de données

<i>app/bio ctrl/authent ID contactless</i>	1
--------------------------------------------	---

L'identifiant doit être enregistré dans une structure TLV.

Identifiant ASCII, données structurée par une suite de « tags »

<i>app/contactless/data format</i>	0
<i>app/contactless/data length</i>	0
<i>app/contactless/data offset</i>	0

L'identifiant de l'utilisateur est utilisé comme clé dans la base de données locale du MorphoAccess® : les empreintes de références associées à cet identifiant sont utilisées lors de l'authentification.

Pour déclencher l'authentification, l'utilisateur doit présenter sa carte au terminal.

**Présentez votre
carte sans contact
s'il vous plaît**



Si l'ID correspondant existe dans la base de données du terminal, l'utilisateur est invité à placer son doigt pour l'authentification biométrique.

**Authentification
Placez votre doigt
s'il vous plaît**



Si l'authentification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

Une fois l'authentification de l'utilisateur effectuée, le terminal attend la présentation d'une nouvelle carte.

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent ID sans contact	Oui	Non	Non	Non	Non	Non

NOTE: Une base de données doit exister dans le terminal.

Identifiant binaire, données non structurées

Authentification sans contact - empreintes dans la base de données	
<i>app/bio ctrl/authent ID contactless</i>	1

Dans ce mode, l'identifiant est lu à un décalage donné sur la carte et est supposé être binaire. Aucune structure TLV n'est requise sur la carte.

Il est possible de définir un identifiant qui n'est pas aligné sur un octet. Cette configuration est utile pour lire des cartes sans contact qui contiennent un identifiant dans une trame Wiegand.

Ce mode peut être utilisé pour utiliser le numéro de série de la carte en tant qu'identifiant.

Identifiant binaire	
<i>app/contactless/data format</i>	1

Les données binaires sont définies par leur position sur le premier bloc de lecture.

La taille de l'identifiant est limitée à 8 octets (*app/contactless/data length 8.0*).

La position de l'identifiant dans le bloc est limitée à l'octet 15 (*app/contactless/data offset 15.0*).

Format de l'identifiant	
<i>app/contactless/B</i>	[1-215] : bloc de lecture
<i>app/contactless/data length</i>	[nombre d'octets].[nombre de bits]
<i>app/contactless/data offset</i>	[nombre d'octets].[nombre de bits]

La manière dont l'identifiant sera interprété est configurable.

Interprétation des données	
<i>app/contactless/data type</i>	0.1 (données binaires, MSB) 0.0 (données binaires, LSB)

L'identifiant de l'utilisateur est utilisé comme clé dans la base de données locale du MorphoAccess® : les empreintes de références associées à cet identifiant sont utilisées lors de l'authentification.

Le déroulement de l'authentification est identique.

Exemple – identifiant 4 octets.

Le terminal est configuré pour lire 4 octets.

Les octets lus sont F4 E1 65 34.

L'identifiant de l'utilisateur correspondant dans la base de données locale est « 4108412212 » (ASCII).

Exemple – lecture du Numéro de Série de la carte (format little endian).

app/contactless/data format = 0.1

app/contactless/data length = 4.0

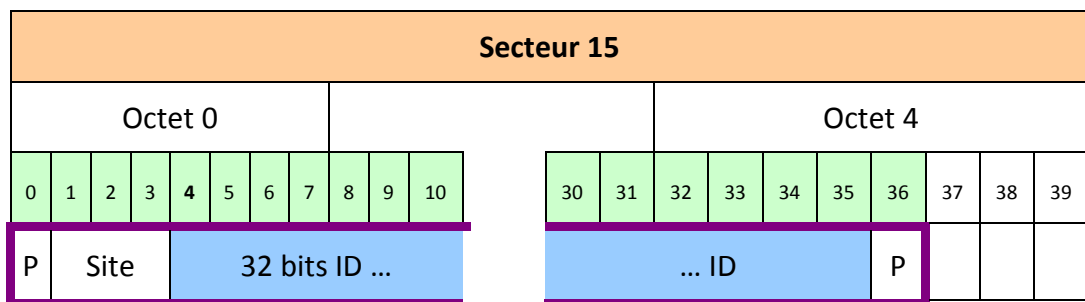
app/contactless/data offset = 0.0

app/contactless/B = 1

Exemple – lecture d'un ID 32 bits stocké dans une trame Wiegand.

Le secteur 15 de la carte contient une trame Wiegand "37 bits" qui contient un ID 32-bits.

Dans cet exemple l'ID commence au quatrième bit et la parité est notée « P ».



La configuration suivante permet d'extraire l'ID de la carte:

<i>app/contactless/data format = 1</i>	ID binaire
<i>app/contactless/data type = 0.1</i>	ID binaire en MSB
<i>app/contactless/data length = 4.0</i>	ID de 4 octets
<i>app/contactless/data offset = 0.4</i>	ID au 4 ^{ème} bit du secteur 15.
<i>app/contactless/B = 46</i>	Lecture au secteur 15

Il est possible de configurer la sortie Wiegand pour recalculer la parité et restituer la trame originale.

Mode d'authentification imposé par la carte

Mode d'authentification imposé par la carte

app/bio ctrl/authent card mode

1

Dans ce mode, la carte décide du type de contrôle à effectuer.

Le tag « CARD MODE » est requis sur la carte. Ce tag peut prendre plusieurs valeurs :

- **PKS** [0x02] : l'identifiant de l'utilisateur et les empreintes doivent être stockés sur la carte. L'authentification biométrique est déclenchée avec les empreintes biométriques. Si un code BIOPIN est présent à la place des empreintes, le BIOPIN est vérifié.
- **ID_ONLY** [0x01] : seul l'identifiant de l'utilisateur est requis. Il n'y a **pas** de contrôle **biométrique**. Cette fonction est utile pour le visiteur qui a besoin d'un accès sans inscription. Mais il est toujours possible d'enregistrer des empreintes sur la carte.
- **PIN_CODE** [0x10] : seul le code PIN est contrôlé.
- **PIN_THEN_PKS** [0x12] : le code PIN puis les empreintes ou le BIOPIN sont contrôlés.

Pour activer ce mode, réglez *app/bio ctrl/authent card mode* sur 1.

Pour désactiver ce mode, réglez *app/bio ctrl/authent card mode* sur 0.

Tags requis sur la carte si la valeur du tag du CARD MODE est PKS.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (PKS)	Oui	Oui	Oui	Oui	Non	Non
authent card mode (PKS) (BIOPIN)	Oui	Oui	Non	Non	Non	Oui

Tags requis sur la carte si la valeur du tag du CARD MODE est ID_ONLY.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (ID_ONLY)	Oui	Oui	Non	Non	Non	Non

Tags requis sur la carte si la valeur du tag CARD MODE est PIN_CODE.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (PIN_CODE)	Oui	Oui	Non	Non	Oui	Non

Tags requis sur la carte si la valeur du tag CARD MODE est PIN_THEN_PKS.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (PIN_THEN_PKS)	Oui	Oui	Oui	Oui	Oui	Non
authent card mode (PIN_THEN_PKS) (BIOPIN)	Oui	Oui	Non	Non	Oui	Oui

La structure de la carte est décrite dans le document *MorphoAccess® Contactless Card Specification*.

Remarque à propos de l'option "bypass" combinée au "card mode"

Quand la clé de configuration *bypass authentication* est activée (voir [Désactivation du contrôle biométrique dans l'authentification](#)), il n'y a aucune vérification de faite (le « card mode » est ignoré).

Remarque concernant le MorphoAccess® avec la licence MA-Xtended chargée

Un MorphoAccess® avec une licence MA-Xtended chargée parcourt les cinq bases de données biométriques pour trouver les empreintes biométriques associées à l'ID saisi.

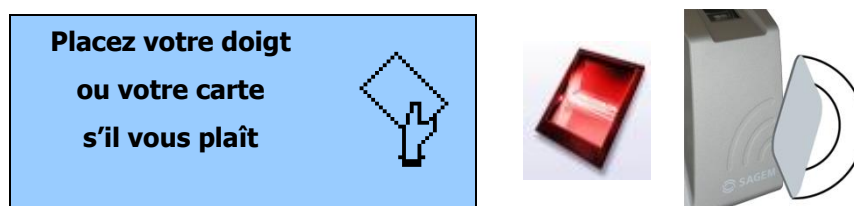
Mode fusionné (ou mode multi-facteur)

Ce mode est la fusion du mode identification et de l'authentification sans contact.

Ce mode permet :

- d'effectuer une identification lorsque l'utilisateur place son doigt (opération identique au mode identification),
- d'effectuer une authentification « sans contact » lorsque l'utilisateur présente sa carte sans contact (opération identique à l'authentification).

Afin de déclencher une des opérations, l'utilisateur doit présenter sa carte devant le terminal ou placer son doigt sur le capteur.



Si l'authentification ou l'identification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

S'il n'y a pas de base de données, la présentation d'une carte sans contact est toujours possible.

L'activation du mode d'identification et d'un mode sans contact active ce mode fusionné.

Mode fusionné (Multi factor)	
<i>app/bio ctrl/identification</i>	1(Activé)
<i>Et</i>	
<i>app/bio ctrl/authent PK contactless</i>	0 (Désactivé) ou 1(Activé)
<i>app/bio ctrl/authent card mode</i>	0 (Désactivé) ou 1(Activé)
<i>app/bio ctrl/authent ID contactless</i>	0 (Désactivé) ou 1(Activé)
<i>app/bio ctrl/control PIN</i>	0 (Désactivé) ou 1(Activé)

Tags requis sur la carte

Le tag requis sur la carte dépend du mode authentification, mais un ID au moins est nécessaire.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentification	Oui	Non	Non	Non	Non	Non

Authentification avec Base Locale- ID saisi à partir du clavier

Authentification biométrique avec un ID saisi à partir du clavier

app/bio ctrl/authent ID keyboard

1

Dans ce mode, l'ID de l'utilisateur est entré sur le clavier du MorphoAccess®. Si l'ID existe dans la base de données (ou dans une des cinq bases de données), le MorphoAccess® effectue une authentification à l'aide des empreintes biométriques associés à cet ID.

ID entré sur le clavier et l'authentification s'effectue



Figure 12: Identifiant utilisateur saisi au clavier

L'écran par défaut invite l'utilisateur à entrer son identifiant numérique.

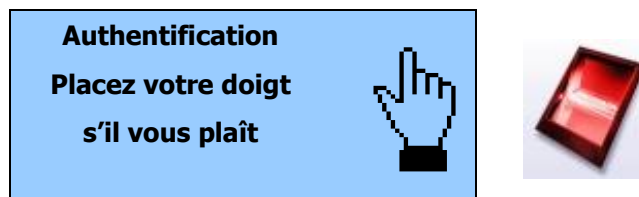


NOTE: La longueur de l'ID est limitée à 24 caractères.

La touche efface le dernier caractère.

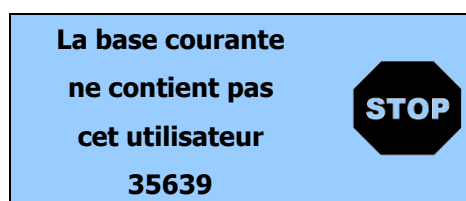
Une fois l'ID saisi, l'utilisateur confirme en appuyant sur la touche .

Si l'ID correspondant existe dans la base de données du terminal, l'utilisateur est invité à placer son doigt pour l'authentification biométrique.



Si l'authentification est réussie, le terminal déclenche l'accès ou renvoie l'ID correspondant au Contrôleur Central.

Si l'identifiant n'est pas présent dans la base de données locale, l'authentification n'est pas lancée.



Une fois l'authentification de l'utilisateur effectuée, le MorphoAccess® attend un nouvel identifiant.

Remarque concernant le MorphoAccess® avec la licence MA-Xtended chargée

Un MorphoAccess® avec une licence MA-Xtended chargée parcourt les cinq bases de données biométriques pour trouver les empreintes biométriques associées à l'ID saisi.

Remarque à propos de l'option "bypass"

Quand la clé de configuration *bypass authentication* est activée (voir [Désactivation du contrôle biométrique](#)), le MorphoAccess® vérifie que l'ID saisi au clavier est présent dans la base locale (ou dans une des cinq bases) avant d'accorder l'accès.

Authentification - ID lu sur l'entrée Wiegand / DataClock

Authentification biométrique : l'ID est lu depuis l'entrée Wiegand ou DataClock

app/bio ctrl/authent remote ID source

1 pour Wiegand

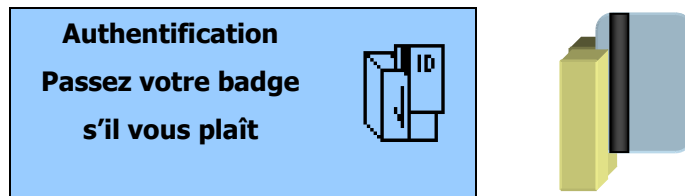
2 pour DataClock

Ce mode requiert un lecteur de carte externe qui envoie l'ID de l'utilisateur sur l'entrée Wiegand ou DataClock du MorphoAccess®.

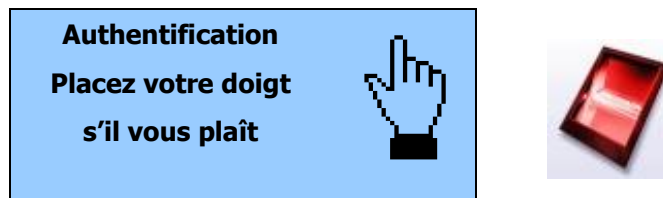


Figure 13: Identifiant utilisateur reçu en Wiegand

L'écran par défaut invite l'utilisateur à présenter son badge afin que le lecteur externe envoie l'ID de l'utilisateur sur l'entrée Wiegand ou DataClock du MorphoAccess®.



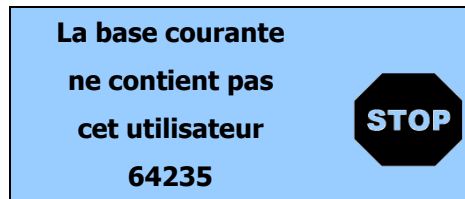
Si l'ID existe dans la base de données, le MorphoAccess® effectue une authentification avec les empreintes biométriques associées à cet ID.



Si l'utilisateur est reconnu, le terminal déclenche l'accès ou renvoie l'ID de l'utilisateur correspondant au Contrôleur Central.

Une fois l'authentification de l'utilisateur effectuée, le MorphoAccess® attend un nouvel identifiant.

Si l'identifiant envoyé par le lecteur n'est pas présent dans la base de données locale, l'authentification n'est pas lancée.



Remarque concernant le MorphoAccess® avec la licence MA-Xtended chargée

Un MorphoAccess® avec une licence MA-Xtended chargée parcourt les cinq bases de données biométriques pour trouver les empreintes associées à l'ID.

Remarque à propos de l'option "bypass"

Quand la clé de configuration *bypass authentication* est activée (voir [Désactivation du contrôle biométrique](#)), le MorphoAccess® vérifie que l'ID envoyé via Wiegand ou Dataclock est présent dans la base locale (ou dans une des cinq bases) avant d'accorder l'accès.

Configuration de la trame Wiegand

Lorsqu'il est configuré pour communiquer avec le protocole Wiegand, le terminal supporte différents formats de données.

Le format par défaut est 26 bits.

Le format de la trame Wiegand est défini selon six clés de configuration. Un protocole différent peut être défini pour l'entrée.

La synchronisation de la trame n'est pas personnalisable. Aucune sécurité supplémentaire (encodage) n'est supportée. Tous les protocoles Wiegand sont réversibles.

Les paramètres personnalisables d'une trame Wiegand sont :

- **Longueur**

Une trame Wiegand peut contenir jusqu'à 128 bits.

- **Bits de contrôle**

Dans une trame Wiegand, les bits de début et de fin sont utilisés comme bits de contrôle. Ils peuvent être fixés à 0 ou à 1 ou être utilisés comme bits de parité (paire ou impaire).

- **Donnée**

Le protocole Wiegand permet de transmettre trois données: le code Site (aussi appelé *Facility Code* ou *Comparison Number*), l'ID utilisateur (aussi appelé *Badge Number* ou *Sequence Number*) et une donnée personnalisable. Les données ont des tailles variables et peuvent être insérées n'importe où dans la trame Wiegand. Les bits de poids fort des données sont insérés en premier.

NOTE: Depuis la version logicielle 2.00, le chemin de cette clé de configuration a été modifié. La valeur de la clé précédente est cependant conservée.

Paramètres de l'entrée Wiegand		
<i>app/wiegand in/</i>		
<i>frame length</i> (avant v2.00 : <i>length</i>)	1-128	Définit le nombre de bits de la trame.
<i>start format</i> (avant v2.00 : <i>start</i>)	0.0 1.0 2.n 3.n 4.0	Définit le bit de contrôle de début de la trame. Reset à 0. Set à 1. Parité paire calculée sur les n premiers bits. Parité impaire calculée sur les n premiers bits. Pas de bit de début.
<i>stop format</i> (avant v2.00 : <i>stop</i>)	0.0 1.0 2.n 3.n 4.0	Définit le bit de contrôle de fin de la trame. Reset à 0. Set à 1. Parité paire calculée sur les n derniers bits. Parité impaire calculée sur les n derniers bits. Pas de bit de fin.
<i>site format</i> (avant v2.00 : <i>site</i>)	n.m	Insert m bits de la valeur site à l'offset n.
<i>ID format</i> (avant v2.00 : <i>ID</i>)	n.m	Insert m bits de la valeur ID à l'offset n.
<i>custom format</i> (avant v2.00 : <i>custom</i>)	n.m	RFU.

Exemple de trame Wiegand (26 bits)

0	1	2	3	...	8	9	10	11	12	...	23	24	25
START	SITE					ID							STOP
1	8 bits					16 bits							1
Données utilisées pour le calcul de la parité START										Données utilisées pour le calcul de la parité STOP			

Désactivation du contrôle biométrique

Une clé de configuration permet de désactiver le contrôle biométrique. Seul l'ID de l'utilisateur est nécessaire. Cet ID peut être lu dans la carte sans contact, saisi au clavier ou reçu via Wiegand/Dataclock.

La clé de configuration *bypass authentication* doit être combinée à un mode d'authentification. L'activation de cette clé signifie que la vérification biométrique est désactivée.

Le terminal contrôle l'existence de l'ID de l'utilisateur dans la base de données

Lorsqu'il est combiné à un mode d'authentification avec lecture des empreintes dans la base de données locale, le MorphoAccess® vérifie que l'identifiant de l'utilisateur est présent sur la base de données locale (ou une des bases locales) avant d'autoriser l'accès.

ID dans la carte sans contact

Désactivation du contrôle biométrique, mais l'ID doit être présent dans la base de données locale	
<i>app/bio ctrl/bypass authentication</i>	1(Activé)
<i>app/bio ctrl/authent ID contactless</i>	1 (Activé)

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentification désactivée	Oui	Non	Non	Non	Non	Non

ID saisi au clavier

Désactivation du contrôle biométrique, mais l'ID doit être présent dans la base de données locale	
<i>app/bio ctrl/bypass authentication</i>	1(Activé)
<i>app/bio ctrl/authent ID keyboard</i>	1 (Activé)

ID reçu via l'entrée Wiegand ou DataClock

Désactivation du contrôle biométrique, mais l'ID doit être présent dans la base de données locale

app/bio ctrl/bypass authentication **1(Activé)**

app/bio ctrl/authent remote ID source 1 pour Wiegand
2 pour DataClock

Le terminal fonctionne comme un simple lecteur de carte sans contact

En activant les clés *app/bio ctrl/bypass authentication* et *app/bio ctrl/authent PK contactless*, le MorphoAccess® autorise toujours l'accès : il fonctionne alors comme un simple lecteur de carte.

Désactivation du contrôle biométrique, l'accès est toujours accordé

app/bio ctrl/bypass authentication **1(Activé)**

app/bio ctrl/authent PK contactless 1 (Activé)

Tags requis sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentification désactivée	Oui	Non	Non	Non	Non	Non

Le terminal lit un ID binaire et fonctionne comme un lecteur de carte

Le MorphoAccess® se comporte comme un simple lecteur de carte sans contact, aucun contrôle biométrique n'est effectué.

Désactivation du contrôle biométrique (le résultat du contrôle biométrique est positif), activation d'un mode d'authentification sans contact	
<i>app/bio ctrl/bypass authentication</i>	1(Activé)
<i>app/bio ctrl/authent PK contactless</i>	1 (Activé)
<i>app/bio ctrl/authent ID contactless</i>	1 (Activé)
Identifiant binaire, données non-structurées	
<i>app/contactless/data format</i>	1 (binary data)

Le terminal lit le numéro de série d'une carte ISO14443-A et fonctionne comme un lecteur de carte

Cette fonctionnalité est disponible à partir de la version de logiciel embarqué V02.09.

Dans cette configuration le MorphoAccess® lit le numéro de série de la carte sans contact (toutes cartes compatibles à la norme ISO14443 type A), et l'envoie sans aucune vérification.

Désactivation du contrôle biométrique (le résultat du contrôle biométrique est positif), activation d'un mode d'authentification sans contact	
<i>app/bio ctrl/bypass authentication</i>	1 (Activé)
<i>app/bio ctrl/authent PK contactless</i>	1 (Activé)
<i>app/bio ctrl/authent ID contactless</i>	1 (Activé)

Le numéro de série de la carte (CARD UID ou CARD SN) est utilisé comme identifiant de l'utilisateur.	
<i>app/contactless/event on</i>	1 (Card UID)
<i>app/bio ctrl/AC_ID</i>	Ajoutez la chaîne "CARDSN:STD;" , ou la chaîne "CARDSN:REV;" si les octets du Card UID doivent être lu dans l'ordre inverse. Retirez la chaîne "CARDDATA;" .

Synthèse des modes de reconnaissance

Le mode de fonctionnement du MorphoAccess® est défini par :

- le mode authentification ou identification requis : Carte seule, Carte + Biométrie, Biométrie seule.
- l'entité qui définit le mode de fonctionnement : Carte ou Terminal.

	Mode défini par Carte <i>app/bio ctrl/authent card mode</i> 1	Mode défini par Terminal <i>app/bio ctrl/authent card mode</i> 0
Mode de fonctionnement		
Authentification Carte seule	ID dans la carte Valeur du tag « CARDMODE » : ID_ONLY	ID dans la carte <i>bypass authent 1</i> <i>authent ID contactless 1</i> Vérification d'ID sur le terminal
		ID dans la carte <i>bypass authent 1</i> <i>authent PK contactless 1</i> Pas de vérification d'ID sur le terminal
Authentification Carte + Biométrie	ID et BIO dans la carte Valeur du tag « CARDMODE » : PKS	ID et BIO dans la carte authentification contournée 0 <i>authent PK contactless 1</i>
		ID sur la carte et BIO dans le terminal authentification contournée 0 <i>authent ID contactless 1</i>

Identification Biométrique seul		ID et BIO dans le terminal <i>identification 1</i>
--------------------------------------------------	--	--------------------------------------------------------------

Réglage de la stratégie de reconnaissance

Mode à deux tentatives

La fonction de reconnaissance du MorphoAccess® offre deux tentatives à l'utilisateur.

En mode identification, si un mauvais doigt est présenté, l'utilisateur a 5 secondes pour présenter à nouveau un doigt. Le résultat du contrôle est envoyé si cette période expire ou si l'utilisateur présente à nouveau un doigt.

En mode authentification, si l'utilisateur présente un doigt non reconnu, il peut replacer son doigt sans présenter à nouveau sa carte. Le résultat du contrôle n'est envoyé qu'après cette deuxième tentative.

Il est possible de régler le délai de présentation d'un doigt et de désactiver ce mode à deux tentatives.

Si le premier contrôle a échoué, le terminal relance un deuxième contrôle avec un algorithme de reconnaissance affiné mais plus lent. Cet algorithme permet la reconnaissance des doigts humides ou mal positionnés.

Paramètres

Par défaut, le mode « deux tentatives » est activé.

Réglage du nombre de tentatives	
<i>app/bio ctrl/nb attempts</i>	1 (une seule tentative) 2 (mode à deux tentatives)

La durée entre deux tentatives en identification peut être modifiée.

Réglage du délai d'identification	
<i>app/bio ctrl/identification timeout</i>	5 (1-60)

En mode authentification, la période de présentation d'un doigt peut être définie.

Réglage du délai d'authentification	
<i>app/bio ctrl/authent timeout</i>	10 (1-60)

Réglage des paramètres de reconnaissance

Réglage du seuil de matching

bio/bio ctrl/matching th 3 (1-10)

Les performances d'un système biométrique sont caractérisées par deux grandeurs : le Taux de Faux Rejet (FRR = False Reject Rate) et le Taux de Fausse Acceptante (FAR= False Acceptance Rate).

Différents compromis sont possibles entre le taux de rejet et le taux de fausse acceptation, en fonction du niveau de sécurité visé pour le système de contrôle d'accès. Quand le confort d'utilisation est recherché, le taux de rejet doit être faible et, à l'inverse, quand la sécurité est recherchée, le taux de fausse acceptation doit être minimisé.

Différents réglages sont proposés dans le MorphoAccess® en fonction du niveau de sécurité visé par le système. La table ci-après détaille les différentes possibilités.

Ce paramètre peut être configuré sur les valeurs de 0 à 10. Ce paramètre spécifie le niveau du seuil de reconnaissance. Les valeurs de ce seuil sont détaillées ci-dessous :

1	Très peu de personnes refusées	TFA < 1 %
2		TFA < 0,3 %
3	Valeur conseillée	TFA < 0,1 %
4		TFA < 0,03 %
5	Seuil intermédiaire	TFA < 0,01 %
6		TFA < 0,001 %
7		TFA < 0,0001 %
8		TFA < 0,00001 %
9	Seuil très élevé (peu de fausses acceptations). Application sécurisée	TFA < 0,0000001 %
10	Seuil élevé uniquement pour des tests	Il y a très peu de mauvaises reconnaissances et beaucoup de refus.

Détection de Faux Doigt (OPTION)

Compatibilité avec les MorphoAccess® Séries 200 et 300 équipés d'un détecteur de faux doigt

Mot de passe

Le mot de passe par défaut est "12345". (Sur les MorphoAccess® Séries 200 et 300, le mot de passe par défaut était "131664".) **Morpho recommande fortement** à l'administrateur de le **modifier**.

Délai après détection de faux doigt

La fonction associée à la clef de configuration `/cfg/Maccess/Security Policy/Delay in 10ms` sur les MorphoAccess® Séries 200 et 300 disparaît.

Niveau de sécurité FFD

La fonction associée à la clé de configuration `app/bio ctrl/FFD security level` ne s'applique qu'aux modes de reconnaissance autonomes. (sur les MorphoAccess® Séries 200 et 300, ce paramètre s'appliquait aussi aux ILVs.) Les ILVs doivent positionner ce paramètre pour obtenir le niveau de sécurité voulu.

Niveau de sécurité Faux Doigt

La détection de faux doigt se caractérise par un taux de faux rejet (pourcentage de vrais doigts détectés comme des faux doigts) et un taux de fausse acceptance (pourcentage de faux doigts détectés comme des vrais doigts). Ce FRR (False Reject Rate = taux de faux rejet) – respectivement FAR (False Acceptance Rate = taux de fausse acceptance) est appelé FFD-FRR – respectivement FFD-FAR. Le taux de rejet global des MorphoAccess® équipés d'un détecteur de faux doigt est donc en fait : $FRR(\text{MorphoAccess}^{\circledast} \text{ standard}) + FFD-FRR$.

On propose trois niveaux de sécurité permettant d'agir sur les paramètres FFD-FRR et FFD-FAR.

0	Niveau de sécurité bas
1 (par défaut)	Niveau de sécurité moyen
2	Niveau de sécurité élevé

Régler le niveau de sécurité FFD

<code>app/bio ctrl/FFD security level</code>	1 (0-2)
----------------------------------------------	---------

Détection de présence

En mode de détection de présence, le capteur est en mode veille en l'absence de détection de présence d'empreinte.

0 (défaut)	Détection de présence standard en mode identification. Le capteur est allumé (état du MorphoAccess® Série 500 sans détecteur de faux doigt)
1	En mode identification, le capteur est en veille (les LEDs sont éteintes) tant qu'aucun doigt n'est détecté

Choisir le type de détection de présence

app/bio ctrl/presence detection 0 (0-1)

ID d'erreur en cas de détection de faux doigt

L'administrateur peut choisir un identifiant spécifique envoyé sur les interfaces Wiegand et DataClock lorsqu'un faux doigt est détecté.

Définir l'identifiant d'erreur FFD

app/failure ID/FFD ID 65535 (0-65535)

Mode veille

Présentation du mode veille

Cette fonctionnalité est disponible depuis la version 2.09 du logiciel embarqué.

Quand ce mode est activé, certaines fonctionnalités sont temporairement désactivées après un laps de temps paramétrable. Cela pour éviter que le MorphoAccess® attire l'attention la nuit, ou pour le rendre moins consommateur d'énergie.

Pour le moment, seules les fonctionnalités suivantes peuvent être désactivées par le mode veille :

- rétro éclairage clavier/écran,
- capteur biométrique.

Ces fonctionnalités peuvent être réactivées à l'aide des fonctionnalités restantes comme les touches du clavier, la réception d'une commande distante, ...

Cela signifie que, si seul le rétro éclairage est désactivé par le mode veille, il peut être activé en posant un doigt sur le capteur allumé, ou en présentant une carte sans contact dans le champ de l'antenne (en fonction de la configuration du terminal).

Activation du mode veille

Le mode veille n'est pas disponible en utilisant le MorphoAccess® en mode proxy.

Ce mode est activé en paramétrant les fonctionnalités à désactiver ainsi que la durée d'inactivité du terminal qui déclenche le mode veille.

Idle Mode	
<i>app/modes/idle peripherals</i>	3 (Désactive le rétro éclairage et le capteur biométrique)
<i>app/modes/idle timeout</i>	0 (Non actif, durée en minutes)

Veillez vous référer à la documentation *MorphoAccess® Parameters Guide* pour plus de renseignements sur le paramétrage du mode veille.

Mode proxy

Le Mode proxy est un mode de fonctionnement dans lequel une application « externe » exécute le contrôle d'accès à distance via les commandes ILV.

Présentation du mode Proxy (ou mode commandé)

Ce mode de fonctionnement permet de contrôler le MorphoAccess® à distance (le lien est IP ou RS422) à l'aide de commandes de gestion de bases de données et de commandes biométriques.

En mode Proxy, le processus de contrôle d'accès est commandé à distance par une application exécutée sur un terminal distant - le MorphoAccess® fonctionne en tant qu'esclave en attente de commandes externes telles que :

- l'identification de l'utilisateur,
- la vérification de l'utilisateur,
- l'activation du relais,
- la lecture des données sur une carte sans contact,
- la gestion de la base de données biométriques,
- les changements de la configuration du terminal,
- la lecture d'une entrée à partir du clavier,
- l'affichage d'un message.

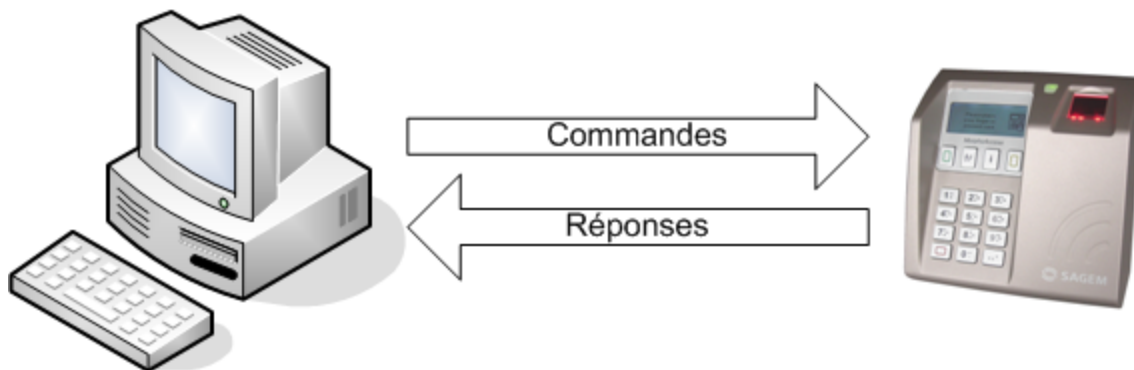


Figure 14: Mode Proxy

Le document *MorphoAccess® Host System Interface Specification* détaille ce mode d'administration.

Pour sécuriser la communication en SSL, voir la documentation *SSL Solution for MorphoAccess®*.

Activation du mode proxy

Dans ce mode, tous les contrôles autonomes (identification, authentifications) sont désactivés : le terminal est en attente d'ordre transmis par un PC distant.

Mode proxy	
<i>app/bio ctrl/identification</i>	0 (Désactivé)
<i>app/bio ctrl/authent card mode</i>	0 (Désactivé)
<i>app/bio ctrl/authent PK contactless</i>	0 (Désactivé)
<i>app/bio ctrl/authent ID contactless</i>	0 (Désactivé)
<i>app/bio ctrl/authent ID keyboard</i>	0 (Désactivé)
<i>app/bio ctrl/authent remote ID source</i>	0 (Aucun)
<i>app/bio ctrl/control PIN</i>	0 (Non)
<i>app/bio ctrl/bypass authentication</i>	0 (Désactivé)

Personnalisation du terminal

Définition d'un contrôle horaire

En mode connecté, une fonction de masque horaire est disponible.

Ce mode autorise l'accès, pour un utilisateur donné, en fonction de plages horaires. Ces plages horaires sont définies par intervalles de 15 minutes sur une semaine.

Chaque utilisateur de la base peut avoir des droits d'accès propres.

NOTE: Depuis la version logicielle 2.00, le chemin de cette clé de configuration a été modifié. La valeur de la clé précédente est cependant conservée.

Activation du masque de temps

>= v2.00 : app/modes/time mask

1(Activé)

< v2.00 : app/time mask/enabled



Cette fonction nécessite de créer une base d'empreinte avec un champ supplémentaire spécifique. Il convient d'activer cette fonction uniquement si la base possède ce champ spécifique.

Pour de plus amples informations, consulter le document *MorphoAccess® Host System Interface Specification*.

Application multilingue

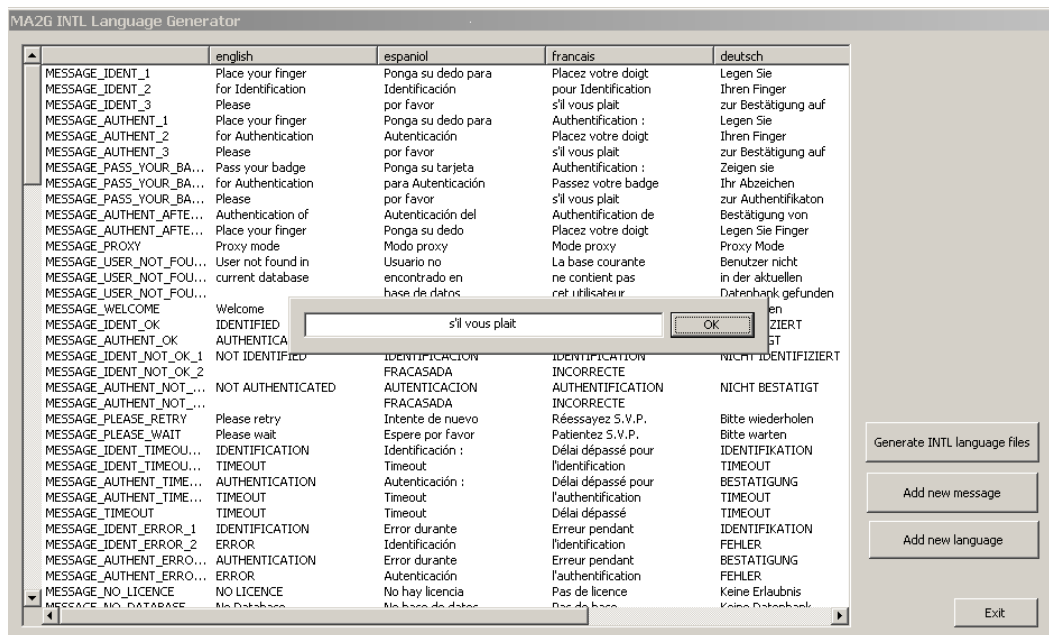
Le MorphoAccess® peut afficher des messages en six langues.

Il est possible de télécharger une table contenant des messages définis par l'administrateur pour rajouter une langue qui ne serait pas livrée avec le terminal..

Pour de plus amples informations sur cette caractéristique, référez-vous aux *MorphoAccess® Host System Interface Specifications*.

Langue par défaut	
<i>app/G.U.I/default language</i>	0 Anglais (défaut)
	1 Espagnol
	2 Français
	3 Allemand
	4 Italien
	5 Portugais
	6 Arabe
	7 Turc

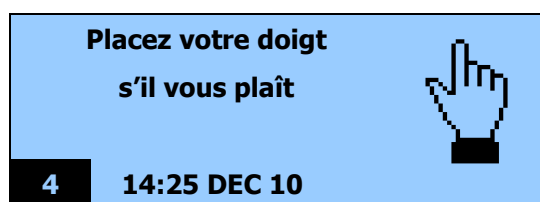
L'outil *Language Customization Tool* permet de redéfinir une table de message et de la télécharger.



Affichage de l'heure

Cette option permet d'afficher l'heure et la date en permanence en bas de l'écran d'accueil.

Affichage de l'heure	
<i>app/G.U.I./display hour</i>	1



Exportation du Résultat du contrôle d'accès

Le MorphoAccess® peut exporter le résultat du contrôle vers un Contrôleur Central ou commander directement un accès. Le résultat peut aussi être enregistré dans un journal local. Cette section présente un aperçu des possibilités qu'offre le MorphoAccess® pour communiquer le résultat d'un contrôle.

Veillez vous référer au document MorphoAccess® Remote Messages Specification qui décrit en détail chaque interface.

Envoi de l'ID au Contrôleur central de Sécurité

Présentation

Le MorphoAccess® peut transmettre le résultat du contrôle vers un Contrôleur Central en utilisant différents protocoles. En fonction du rôle du Contrôleur dans le système celui-ci va pouvoir autoriser l'accès ou afficher un message.

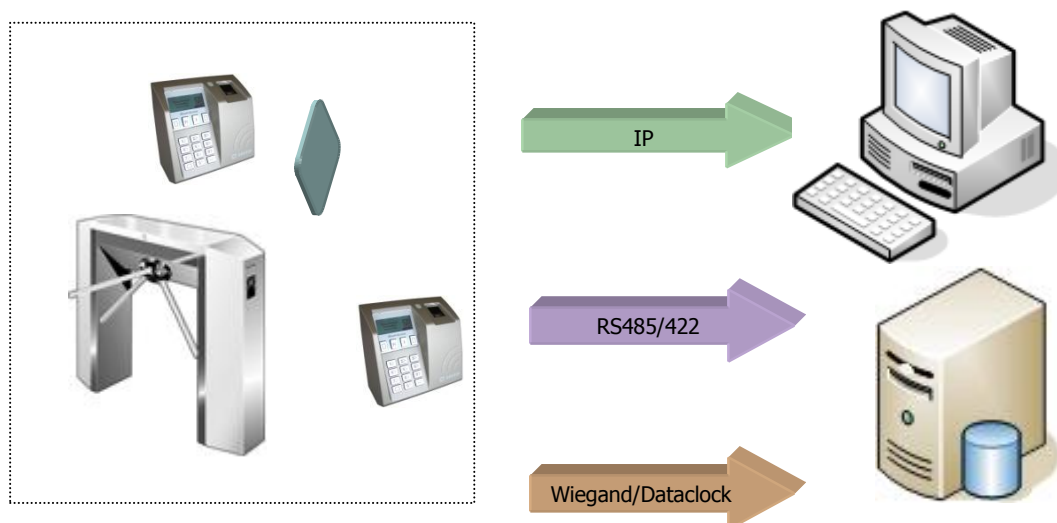


Figure 15: Envoi du résultat du contrôle d'accès

Le document *MorphoAccess® Remote Messages Specification* décrit les différentes configurations proposées par le MorphoAccess® pour dialoguer avec un contrôleur et comment les utiliser.

Protocoles supportés

Le terminal peut transmettre le résultat du contrôle à un contrôleur via les protocoles suivants :

- Wiegand,
- Dataclock,
- RS485/422,
- IP (TCP ou UDP ou SSL).

Pour l'utilisation de SSL, veuillez vous référer au document *SSL Solution for MorphoAccess®*.

Activation du relais

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

Activation du relais	
<i>app/relay/enabled</i>	1 (Activé)

La durée d'ouverture du relais peut être définie. Par défaut le relais s'activera pendant 3 secondes.

Temps d'ouverture du relais en 10 ms	
<i>app/relay/aperture time in 10 ms</i>	300 (50 à 60 000)

L'état par défaut du relais peut être paramétré. Par défaut, le relais est ouvert lorsqu'il n'est pas commandé (pas de contrôle réussi).

État par défaut du relais	
<i>app/relay/default state</i>	0 (ouvert) 1 (fermé)



Ce type d'installation offre un faible niveau de sécurité.

Commande déportée du relais

Cette fonctionnalité est disponible à partir de la version de logiciel embarqué V02.07.

L'entrée LED1 du MorphoAccess® permet d'activer le relais

app/relay/external control by LED1

1 (activé)

Cette fonction permet d'activer le relais avec un interrupteur connecté sur l'entrée LED1 du MorphoAccess®. Dès lors le relais peut être activé suite à un contrôle biométrique réussi ou via un signal sur l'entrée LED1.

- Si LED1 est en haute impédance (interrupteur ouvert) le relais ne s'active pas.
- Si LED1 est connecté à GND (interrupteur fermé) le relais s'active selon les paramètres détaillés ci-dessus.

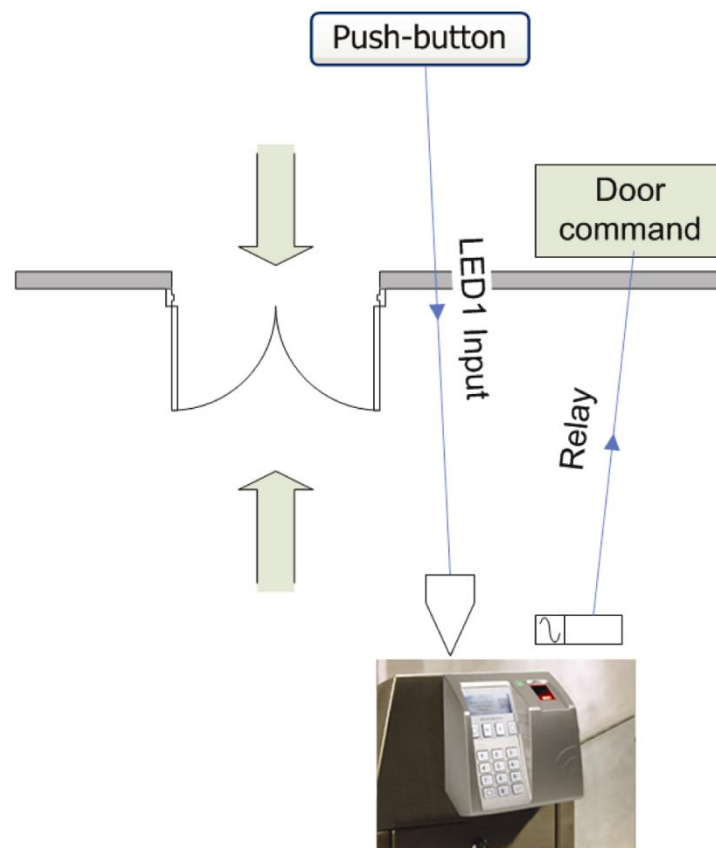


Figure 16: Activation du relais interne par signal LED1

Dans une installation type le MorphoAccess® peut contrôler la gâche de la porte avec son relais :

- un contrôle biométrique réussi permet d'accéder au bâtiment,

- un interrupteur connecté à l'entrée LED1 ouvre la porte pour quitter le bâtiment.

Fichier journal

Le MorphoAccess® enregistre le résultat d'un passage

app/log file/enabled

1

Le MorphoAccess® peut sauvegarder une trace des événements de contrôle d'accès dans un journal local.

Il sauvegarde :

- la date et l'heure de l'enregistrement,
- le résultat du contrôle d'accès (accepté ou refusé, et la raison si refusé),
- l'ID de l'utilisateur (si disponible),
- et éventuellement une information de pointage.

Le terminal MorphoAccess® Série 500 peut enregistrer jusqu'à 65000 évènements.

Il est possible de télécharger le fichier journal. Les fonctions d'administration de ce fichier sont décrites dans le document *MorphoAccess® Host System Interface Specification*.

Il est également possible de consulter le fichier journal à l'aide de l'application *Logs Viewer*.

8 JANVIER 2007
15:25,OK,783170
15:28,KO,
15:45,OK,7895641
15:59,KO,783170

L'outil « *MAGetLog* » fourni sur le CDROM d'installation permet de télécharger ce fichier.

Actions spécifiques lorsque le journal est plein

app/log file/full handling

"00000000" (pas d'action)

Selon la configuration, lorsque la limite du journal est atteinte, le terminal peut :

- Envoyer un message d'information à un hôte distant (cf. [Envoi de messages](#))
- Afficher un message sur l'écran
- Effacer le fichier journal.

Veillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails.

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 de résultat du contrôle d'accès ».

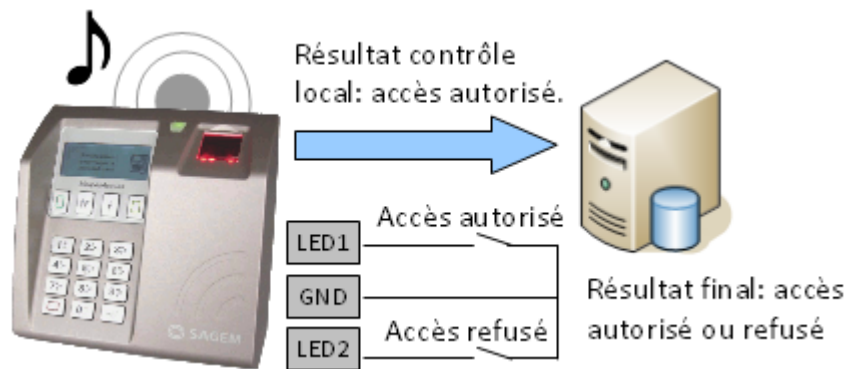


Figure 17 : Fonctionnalité LED IN

Merci de consulter le guide d'installation de votre terminal MorphoAccess® 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)

Fonctions de Sécurité

Détection d'intrusion et d'arrachement

Activation de l'alarme

Le MorphoAccess® comporte deux capteurs permettant de détecter :

- une tentative d'arrachement (le capteur optique se déclenche),
- une tentative d'intrusion (l'interrupteur anti-intrusion se déclenche).

Lorsque l'un des deux capteurs s'active, il est possible d'envoyer un message d'information sur les sorties standard vers le Contrôleur Central.

Il est aussi possible de lire un signal directement sur le bornier (boucle sèche).

NOTE: Les deux capteurs sont en série – on ne peut pas distinguer le type d'intrusion. Veuillez vous référer au *Manuel d'installation* pour identifier ces interrupteurs sur le terminal.



Figure 18: Détection intrusion ou arrachement

Pour envoyer un message en cas d'intrusion (IP, RS485/RS422, Wiegand, DataClock), l'interface correspondante doit être activée sinon aucune alarme ne sera envoyée.

Wiegand et Dataclock sont multiplexés sur les mêmes lignes, ces protocoles doivent être activés un par un ; la priorité est donnée au Wiegand, puis au Dataclock.

Ces interfaces sont activées par les clés de configuration suivantes :

- app/send ID wiegand/enabled,
- app/send ID dataclock/enabled,
- app/send ID serial/enabled,
- app/send ID serial/mode (pour sélectionner le lien RS422 ou RS485),
- app/send ID UDP/enabled,

- `app/send ID ethernet/mode`,
- `app/send ID ethernet/SSL enabled`.

Pour utiliser le SSL sur le MorphoAccess®, veuillez vous référer à la documentation *SSL Solution for MorphoAccess®*.

Régler la clé `app/tamper alarm/level` sur une valeur appropriée configure la fonction de gestion des interrupteurs de sécurité.

Niveau d'alerte du dérangement	
<code>app/tamper alarm/level</code>	0 (0 – 2)
<p>0 Aucune alerte.</p> <p>1 Envoi d'un message (pas d'alarme sonore).</p> <p>2 Envoi d'un message et activation d'une alarme sonore.</p>	

La clé `app/failure ID/alarm ID` définit la valeur de l'ID d'alerte à envoyer sur les sorties Wiegand ou DataClock. Cet ID doit être distinct d'un ID d'utilisateur ou d'un autre ID d'erreur. Pour être validée, la clé `app/failure ID/enabled` doit être réglée sur 1.

ID d'alerte associé à l'événement « intrusion »	
<code>app/failure ID/alarm ID</code>	65535 (0 – 65535)
<code>app/failure ID/enabled</code>	1

Sur les sorties Wiegand ou DataClock, l'ID d'alerte est envoyé comme d'autres ID d'échec.

Exemples

Exemple 1 : Envoyer l'ID n°62221 par l'interface Wiegand et émettre une alerte sonore en cas de détection d'intrusion.

Pour envoyer une alerte sur l'interface Wiegand, la clé `app/send ID wiegand/enabled` prend la valeur 1 et la clé `app/tamper alarm/level` la valeur 2.

La clé `app/failure ID/alarm ID` doit être réglée sur 62221 pour lier l'événement d'intrusion à cet identifiant.

Enfin la clé `app/failure ID/enabled` est positionnée à 1 pour activer l'envoi de messages d'erreurs sur la sortie Wiegand.

Exemple 2 : Envoyer une alerte silencieuse en UDP en cas de détection d'intrusion.

Pour envoyer une alerte dans UDP, la clé `app/send ID UDP/enabled` doit être réglée sur 1.

Puis la clé *app/tamper alarm/level* doit être réglée sur 1 (alerte silencieuse).

Mots de passe

Deux mots de passe protègent le système :

- le *Terminal Configuration Password* verrouille l'accès à la configuration du MorphoAccess®,
- le *User Management Password* est nécessaire pour avoir accès à la base de données locale : il protège les applications d'Enrôlement Local et de Visualisation des Événements de Contrôle d'Accès.



Les valeurs par défauts des mots de passe sont « 12345 ».



Si un mot de passe est perdu, le terminal doit être retourné au SAV de Morpho.

Envoi de messages

Cette section décrit comment le terminal MorphoAccess® Série 500 peut envoyer des messages à un hôte distant. Ces messages détaillés ci-après sont différents de ceux du chapitre émission du résultat (cf. [Exportation du Résultat](#)).

Principe

Lorsque des évènements prédéfinis surviennent Durant le fonctionnement de l'application de contrôle d'accès, des messages d'informations peuvent être générés et envoyés à un hôte distant.

Ces évènements prédéfinis sont :

- Fichier de journal plein
- Demande de synchronisation de la base biométrique

Veillez vous référer au document *MorphoAccess® Remote Messages Specification* pour plus de détails concernant le contenu des messages.

ÉVÈNEMENTS

L'envoi de messages sur évènements est paramétrable à l'aide de deux fichiers de configuration :

- Events.cfg
- Remotemsg.cfg

Cette section détaille uniquement le fichier events.cfg.

La configuration permet de choisir les évènements qui génèrent un envoi de message. Par défaut, tous les évènements prédéfinis génèrent un envoi.

Masque d'évènements prédéfinis	
<i>Events/general/active</i>	"FFFFFFF" (Tous les évènements génèrent un envoi)

Pour chaque évènement, le nombre d'envoi du message est configurable :

Nombre d'envoi pour l'évènement "Journal interne plein"	
<i>Events/log_full/nb sending</i>	0 (Pas de tentative d'envoi)

Pour chaque envoi, les paramètres suivants peuvent être réglés :

- Nombre de ré-essais pour l'envoi courant,
- Temps entre deux essais,
- Réponse attendue par le terminal ou non,
- Interface d'envoi du terminal (cf. Interfaces d'envoi).

Veillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails à propos de la configuration pour l'envoi de messages.

Interfaces d'envoi

Cette section décrit uniquement le fichier `remotemsg.cfg`.

La configuration du terminal MorphoAccess® permet de définir le nombre d'interfaces disponibles pour l'envoi de messages (cf. Évènements).

Par défaut, aucune interface n'est disponible.

Nombre d'interfaces disponibles	
<code>Remotemsg/interface/nb interfaces</code>	0

Pour chaque interface disponible, les paramètres suivants peuvent être réglés :

- Lien de communication
- Protocole utilisé
- Paramètres dépendant du lien de communication et du protocole choisis.

Seul le lien IP et le protocole TCP sont disponibles. Dans ce cas, les paramètres sont :

- L'adresse IP de l'hôte distant (i.e. celui qui va recevoir le message)
- Le port de l'hôte distant
- Le timeout pour l'envoi de données
- Le timeout pour la réception de données

Veuillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails concernant la configuration des interfaces.

Annexes

Enrôlement sur terminal avec synchronisation

Principe

En fonction de sa configuration, le terminal MorphoAccess® peut enregistrer chaque action effectuée sur une base de données biométriques à l'aide de l'application d'enrôlement local.

Par la suite, un administrateur peut exporter ces changements sur d'autres MorphoAccess® mais en gardant la base de donnée de référence sur la station d'enrôlement (typiquement MEMS™).

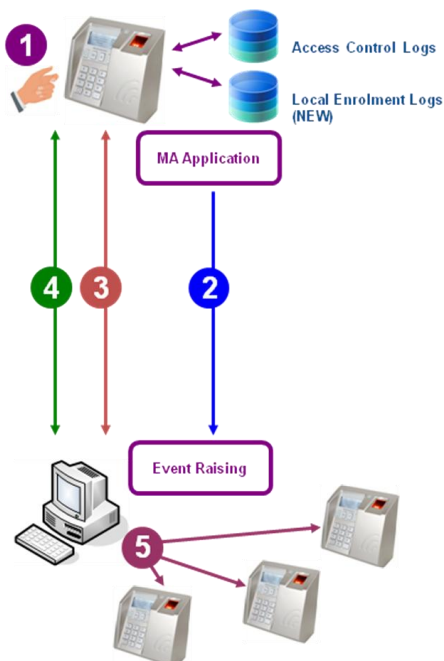
Sur demande de l'administrateur, le terminal envoie un message de synchronisation à la station d'enrôlement (cf. [Envoi de messages](#)).

La station d'enrôlement demande les changements effectués par analyse des enregistrements de l'application d'enrôlement local, puis mets à jour sa base de données en demandant les données des personnes ajoutés au terminal par exemple.

Enfin, la station d'enrôlement mets à jour les bases de données de tous les MorphoAccess® et efface le fichier d'enregistrement de l'application d'enrôlement local du terminal de départ.

Note: Le fichier d'enregistrement contenant les changements de la base de données n'est pas celui qui contient les événements de contrôle d'accès.

Exemple avec MEMS™ :



1

L'administrateur local ajoute/modifie/efface des utilisateurs ou encode des badges sans contacts, ce qui génère autant de lignes dans le fichier d'enregistrement. A la fin de la session d'enrôlement, il demande une synchronisation.

2

Le terminal redémarre et envoie la demande à la station d'enrôlement.

3

MEMS acquitte le message de synchronisation. Et demande les lignes du fichier d'enregistrements.

4

Puis l'application MEMS demande les données des utilisateurs qu'elle souhaite importer. Le terminal envoie les données (y compris les données biométriques). La base de données de MEMS est mise à jour.

5

MEMS met à jour tous les terminaux avec cette nouvelle base de données. Enfin MEMS efface le fichier d'enregistrement du terminal de départ.

Activation

Pour activer cette fonctionnalité, plusieurs paramètres doivent être réglés :

- Les actions à enregistrer (clé `/log/LogParam/LogMask`),
- Le nom du fichier d'enregistrements (clé `/log/LogParam/LogFile`)
- La taille du fichier d'enregistrements (clé `/log/LogParam/LogFileSize`),
- Les évènements qui génèrent des envois de messages (clé `/events/general/active`),
- Le nombre de message de synchronisation (clé `/events/bio_chg/nb sending`),
- Les paramètres de l'envoi (clé `/events/bio_chg/send#`) cf. [Évènements](#)
- L'interface d'envoi (clé `/remotemsg/interfaces/int#`) cf. [Interfaces d'envoi](#)

Veillez vous référer au document *MorphoAccess® Parameters Guide* pour en savoir plus sur ces clés de configuration, et au document *MorphoAccess® Enrolment Application User Guide* pour en savoir plus sur les différentes actions à enregistrer.

Une fois la configuration effectuée, l'item "Synchronize" apparaît dans le menu de l'application d'enrôlement local.

Arrêt

La synchronisation ne peut pas être annulée. La procédure s'arrête lorsque la station d'enrôlement a confirmé la réception du message de synchronisation, ou lorsque le nombre maximal de tentatives pour envoyer la demande de synchronisation a été atteint.

Compatibilité avec la gamme MorphoAccess® 220 / 320

Ces tableaux présentent les équivalences de configuration entre les MorphoAccess® Séries 200 et 300 et le MorphoAccess® Série 500.

Le mode multi-facteurs (ou mode fusionné) (*/cfg/Maccess/Admin/mode 5* sur 220 et 320) est activé lorsque *app/bio ctrl/identification* vaut « 1 » et un des modes sans contact est activé

MA Série 200/300	MA Série 500
------------------	--------------

Identification

<i>/cfg/Maccess/Admin/mode 0</i>	<i>app/bio ctrl/identification 1</i>
----------------------------------	--------------------------------------

Authentification sans contact - ID sur la carte, empreintes dans la base de données locale

<i>/cfg/Maccess/Admin/mode 4</i>	<i>app/bio ctrl/authent ID contactless 1</i>
----------------------------------	----------------------------------------------

Authentification sans contact : mode carte (la carte décide du déroulement du contrôle)

<i>/cfg/Maccess/Contactless/without DB mode 0</i> <i>/cfg/Maccess/Admin/mode 3 or</i>	<i>app/bio ctrl/authent card mode 1</i>
<i>/cfg/Maccess/Admin/mode 5</i> <i>(mode à multiples facteurs)</i>	<i>app/bio ctrl/identification 1</i>

Authentification sans contact - ID et empreintes sur la carte

<i>/cfg/Maccess/Contactless/without DB mode 2</i> <i>/cfg/Maccess/Admin/mode 3 or</i>	<i>app/bio ctrl/authent PK contactless 1</i>
<i>/cfg/Maccess/Admin/mode 5</i> <i>(mode à multiples facteurs)</i>	<i>app/bio ctrl/identification 1</i>

Authentification sans contact - ID « seul », pas de vérification biométrique	
<i>/cfg/Maccess/Contactless/without DB mode 1</i> <i>/cfg/Maccess/Admin/mode 3 or</i>	<i>app/bio ctrl/authent PK contactless 1</i> <i>app/bio ctrl/bypass authentication 1</i>
<i>/cfg/Maccess/Admin/mode 5</i> <i>(mode à multiples facteurs)</i>	<i>app/bio ctrl/identification 1</i>

Authentification : ID lu partir de Wiegand ou DataClock	
<i>/cfg/Maccess/Admin/mode 1</i>	<i>app/bio ctrl/authent remote ID source 1 or 2</i>
Configuration des cavaliers définissant la source de l'ID (DataClock ou Wiegand)	

Mode proxy	
<i>/cfg/Maccess/Admin/mode 2</i>	<i>app/bio ctrl/identification 0</i> <i>app/bio ctrl/authent card mode 0</i> <i>app/bio ctrl/authent PK contactless 0</i> <i>app/bio ctrl/authent ID contactless 0</i> <i>app/bio ctrl/authent ID keyboard 0</i> <i>app/bio ctrl/control PIN 0</i> <i>app/bio ctrl/bypass authentication 0</i> <i>app/bio ctrl/authent remote ID source 0</i>

Synthèse des modes avec carte sans Contact

Opération	Authent card mode	Authent PK contactless	Authent ID contactless	Bypass authentication
Authentification - empreintes dans la base de données Lecture de l'ID sur la carte sans contact. Récupération des empreintes correspondantes dans la base de données. Authentification biométrique à l'aide de ces empreintes. Envoi de l'ID si l'authentification est réussie.	0	0	1	0
Authentification - empreintes sur la carte Lecture de l'ID et des empreintes sur la carte sans contact. Authentification biométrique à l'aide de ces empreintes. Envoi de l'ID si l'authentification est réussie.	0	1	0	0
Authentification – en fonction du mode de la carte Lecture du mode de la carte, de l'ID, des empreintes (si nécessaire par le mode carte) sur la carte sans contact. Si le mode carte est « ID seul », envoi de l'ID. Si le mode carte est « Authentification », authentification biométrique à l'aide des empreintes stockées sur la carte, puis envoi de l'ID si l'authentification est réussie.	1	0	0	0
Authentification - empreintes dans la base de données – contrôle biométrique désactivé Lecture de l'ID sur la carte sans contact. Vérification de la présence des empreintes correspondant dans la base de données. Envoi de l'ID si les empreintes sont présentes.	0	0	1	1
Authentification - empreintes sur la carte – contrôle biométrique désactivé Lecture de l'ID sur la carte sans contact. Envoi de l'ID.	0	1	0	1
Authentification en mode « carte » – contrôle biométrique désactivé Lecture du mode de la carte, de l'ID, des empreintes (si nécessaire par le mode carte) sur la carte sans contact. Quelque soit le mode de la carte, envoi de l'ID.	1	0	0	1

Tags requis sur la carte sans contact

Opération	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentification avec empreintes dans la base de données	Oui	Non	Non	Non	Non	Non
Authentification avec les empreintes sur la carte	Oui	Non	Oui	Oui	Non	Non
Authentification en mode carte (ID_ONLY)	Oui	Oui	Non	Non	Non	Non
Authentification en mode carte (PKS)	Oui	Oui	Oui	Oui	Non	Non
Authentification avec les empreintes dans la base de données – contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non
Authentification avec les empreintes dans la carte – contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non
Authentification en mode carte (ID_ONLY) – contrôle biométrique désactivé	Oui	Oui	Non	Non	Non	Non
Authentification en mode carte (PKS) – contrôle biométrique désactivé	Oui	Oui	Oui	Oui	Non	Non
Vérification du code BIOPIN	Oui	Non	Non	Non	Non	Oui
Vérification du code PIN	Oui	Non	Non	Non	Oui	Non

Documentations

Informations à l'attention de l'administrateur

Manuel utilisateur MorphoAccess® Série 500

Ce document décrit les modes de fonctionnement et les paramètres du terminal.

MorphoAccess® 500 Series Configuration Application User Guide

Détaille l'application de configuration du terminal.

MorphoAccess® Parameters User Guide

Ce document fournit la liste des clés de configurations du terminal et leur valeur par défaut.

MorphoAccess® 500 Series Enrolment Application User Guide

Décrit l'application d'enrôlement local.

MorphoAccess® 500 Series Log Viewer User Guide

Détaille l'application de visualisation des événements de contrôle d'accès.

Informations à l'attention de l'installateur

Manuel d'Installation MorphoAccess® Série 500

Ce document décrit les interfaces électriques et les procédures de connexion du terminal.

Informations à l'attention du développeur

MorphoAccess® Host System Interface Specification

Description complète des commandes de gestion à distance

MorphoAccess® Remote Messages Specification

Détaille la manière dont le MorphoAccess® envoie le résultat du contrôle d'accès à un Contrôleur Central.

MorphoAccess® Contactless Card Specification

Décrit les caractéristiques du contenu de la carte sans contact

Outils de support

USB Network Tool User Guide

Manuel utilisateur de l'outil de configuration du réseau, via la clé USB

MorphoAccess® Upgrade Tools User Guide

Présentation des outils de mise à jour des logiciels

License Manager User Guide

Détaille la procédure de chargement d'une licence dans le MorphoAccess® Série 500.

Support

FAQ

Le capteur est éteint

Vérifier que la base contient au moins un enregistrement.

Vérifier que l'identification est activée.

Le terminal retourne des réponses aléatoires à des envois de « Ping »

Vérifier le masque de sous-réseau. Demandez la bonne valeur à votre administrateur.

Contacts

Service client

Morpho

SAV Terminaux Biométriques
Boulevard Lénine - BP428
76805 Saint Etienne du Rouvray
FRANCE
Tél: +33 02 35 64 55 05

Hotline

Morpho

Support Terminaux Biométriques
18, Chaussée Jules César
95520 Osny – FRANCE
hotline.biometrics@t.my-technicalsupport.com

Tél. : + 33 1 58 11 39 19

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

www.biometric-terminals.com

Pour accéder à ce service, veuillez prendre contact avec nous afin d'obtenir votre identification.

Merci de nous faire parvenir un email plutôt que d'appeler la ligne d'assistance.

Copyright ©2012 Morpho

<http://www.morpho.com/>



Siège social : Le Ponant de Paris
27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE