MorphoAccess® Série 100

Manuel Utilisateur

Produced by Morpho

http://www.morpho.com/

Table des matières

Table des illustrations

Historique du document

Date	Description
Juillet 08	Ajout de la fonctionnalité « juvénile » des MA2xx et MA3xx.
	Ajout de la fonctionnalité utilisation du « Card UID » d'une carte sans contact compatible ISO1443 type A, comme ID utilisateur.
Juin 09	Ajout des terminaux DESFire®
Octobre 09	Ajout de l'envoi de messages
Février 11	Remplacement du nom et du logo de la société
Juin 2011	Amélioration description de la fonction LED IN (LED1 & LED2)
Février 2012	Ajout du support des cartes DESFire® EV1 AES Ajout du support de 65000 enregistrements de transactions

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 à l'aide de la vérification 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 (MorphoSoft™ et MorphoImaging™). Cette technologie est basée sur une expérience de 20 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.

Objet du document

Ce guide s'adresse aux utilisateurs de terminaux MorphoAccess® de la série 100.

« MorphoAccess® Série 100 » est une appellation générique qui regroupe les terminaux MorphoAccess® appartenant à la série MA 100. La liste des produits correspondants est détaillée dans le tableau ci-dessous.

		Capteur biométrique	**Lecteur de cartes sans contact**		
			iCLASS®	**MIFARE®**	**DESFire®**
Série MA 100	MA 100	√			
	MA 110	√	√		
	MA 120	√		√	
	MA 120 D	√		√	√

Instructions de sécurité

L'installation de ce produit doit être effectuée par du personnel qualifié et doit être conforme aux dispositions locales.

Il est fortement recommandé d'utiliser une alimentation de classe II de 12 V ±5 % et 0,5 A. min selon Safety Electrical Low Voltage (SELV) La longueur du câble d'alimentation 12 V ne doit pas excéder 5 mètres.

Ce produit est conçu pour une installation avec une alimentation conforme à la norme EN60950, selon les spécifications NEC Classe 2, ou fourni par une alimentation externe EN60950 de Classe 2, source limitée ou LPS et notée 12 Vcc, 0,5 A minimum.

En cas de connexion bloc à bloc, il est recommandé de connecter 0 V à la terre. Le câble de masse doit être connecté avec le bloc terminal 0 V GND.

Informations pour l'Europe

Morpho déclare par la présente que le MorphoAccess® a été testé et s'est avéré conforme aux normes ci-dessous, conformément à la Directive EMC 89/336/EEC : EN55022 (1994) / EN55024 (1998), EN300-330 (1999) et à la Directive basse tension 73/23/EEC modifiée 93/68/EEC : EN60950 (2000).

Informations pour les États Unis d'Amérique

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

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

Responsable : **Morpho** , Le Ponant de Paris, 27, rue Leblanc – F 75512 PARIS CEDEX 15 – FRANCE.

NOTE: Cet équipement a été testé et jugé conforme aux limites pour un dispositif numérique Classe B, 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 résidentielle. 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.

Cependant, il n'y a aucune garantie qu'aucune interférence ne se produira dans une installation particulière. Si cet équipement provoque des interférences dangereuses lors de la réception de la télévision ou de la radio, pouvant être déterminé par la mise hors ou en tension de l'équipement, l'utilisateur est encouragé à essayer de corriger l'interférence par une ou plusieurs des mesures suivantes :

réorienter ou déplacer l'antenne de réception,

augmenter la distance entre l'équipement et le récepteur,

brancher l'équipement à l'intérieur d'une sortie sur un circuit différent de celui sur lequel le récepteur est branché,

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

Informations pour le Canada

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Présentation du terminal MorphoAccess® Série 100

Présentation des interfaces

Interface homme-machine

Le terminal MorphoAccess® Série 100 présente une interface homme-machine simple et ergonomique dédiée au contrôle d'accès sur la base de la reconnaissance des empreintes digitales :

- scanner optique de haute qualité pour relever les empreintes (1),
- LED multi couleur (8 couleurs) (2),
- « Buzzer » multi ton (3),

lecteur sans contact optionnel pour lire des empreintes de référence depuis une carte sans contact (iCLASS®, MIFARE®, ou DESFire® selon le modèle de MorphoAccess®) (4).

Figure 1 : Face avant du terminal MorphoAccess® Série 100

Interfaces électriques

Le terminal présente de multiples interfaces dédiées aux informations de gestion et de contrôle :

- sortie multiplexée Wiegand / Dataclock / RS485 (5),
- deux entrées LED IN pour améliorer l'intégration dans un système de contrôle d'accès (6),
- relais pour commander directement un accès (7),
- détection d'intrusion (déverrouillage du socle) (8),
- interface Ethernet (10/100 Mbits/s) pour la gestion à distance via TCP/SSL et l'envoi du résultat de contrôle via UDP/TCP/SSL (9),
- port hôte USB dédié à la configuration locale (10).

Figure 2 : Bornier du terminal MorphoAccess® Série 100

Le *Manuel d'installation* décrit précisément chaque interface et chaque procédure de connexion.

Synoptique d'un système de contrôle d'accès

Architecture type

Architecture type comprenant un MorphoAccess®, une Station d'Enrôlement, et un Contrôleur Central

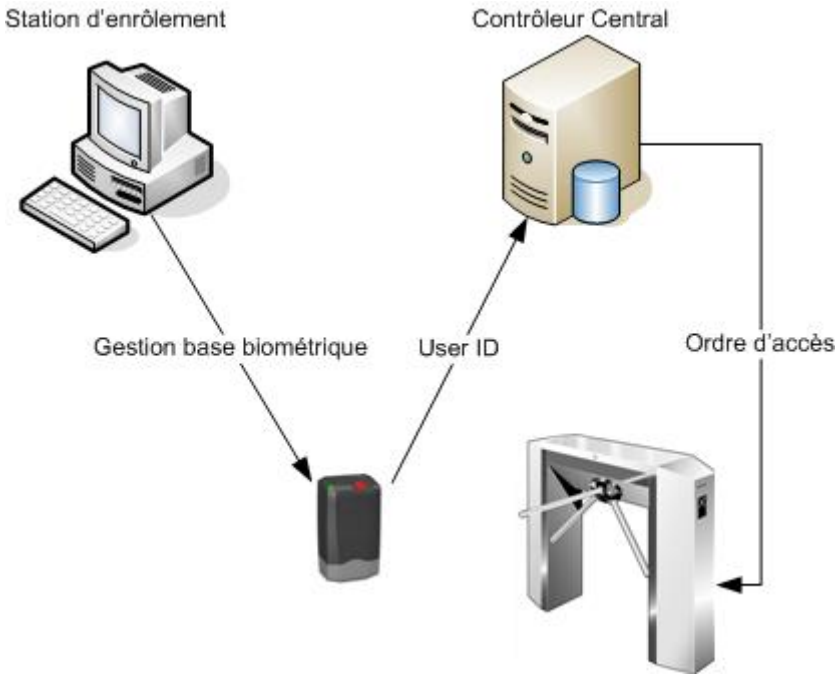


Figure 3 : Système de contrôle d'accès typique

Gestion de la base de données biométriques du MorphoAccess® Série 100

La gestion de la base de données biométrique interne du MorphoAccess® peut être effectuée à distance par une Station d'Enrôlement (généralement MEMS™).

Mode de fonctionnement du MorphoAccess®

Le MorphoAccess® fonctionne selon deux modes exclusifs.

- En Mode Autonome, la base de données biométriques peut être gérée par une Station d'Enrôlement et téléchargée dans le MorphoAccess®.
- En Mode Proxy, le terminal est commandé par une application distante qui envoie des commandes 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, ou non.

Présentation du contrôle d'accès

Le MorphoAccess® fonctionne selon deux modes de reconnaissance biométrique : identification ou authentification. Les deux modes peuvent être activés simultanément (mode fusionné).

Identification

L'utilisateur pose un doigt sur le capteur biométrique, et le terminal se charge de trouver l'identifiant correspondant.

En mode identification, la procédure démarre lorsqu'un doigt est sur le capteur biométrique.

L'empreinte digitale relevée est comparée à toutes celles de la base de données d'empreintes numérisées – « 1 contre N ».

Le terminal peut enregistrer jusqu'à 500 utilisateurs (2 doigts par utilisateur) dans sa base de données locale.

Dans ce mode, le capteur est toujours activé, en attente de la présentation d'un doigt.

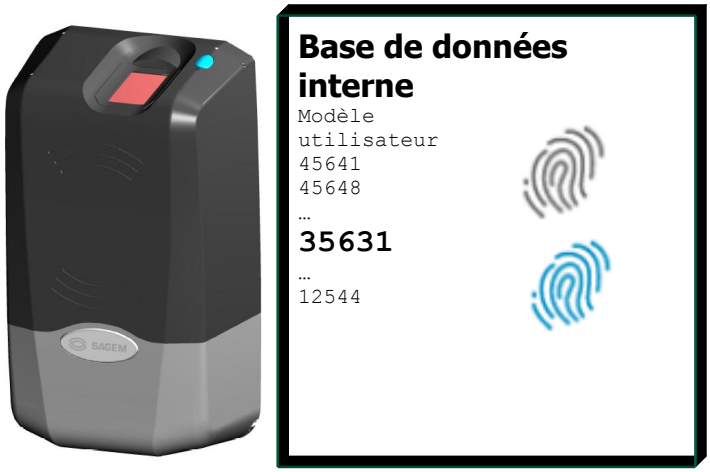


Figure 4 : Mode Identification

Lorsque l'utilisateur est reconnu (son empreinte de référence est dans la base), l'accès est autorisé.

Lorsque l'utilisateur n'est pas reconnu (son empreinte de référence n'est pas dans la base), l'accès est refusé.

Voir la section Contrôle d'accès par identification.

Authentification

L'utilisateur fournit son identifiant et le terminal se charge de le vérifier en comparant l'empreinte relevée à une empreinte de références.

En mode authentification, la procédure démarre lorsque l'identifiant est fourni.

Authentification avec empreintes de références dans une carte sans contact (1 versus 1)

Les empreintes digitales numérisées d'un utilisateur sont stockées sur une carte sans contact de type iCLASS®, MIFARE® ou DESFire®.

Figure 5 : Mode Authentification

Lorsque l'utilisateur est reconnu (son empreinte de référence est dans la base), l'accès est autorisé.

Lorsque l'utilisateur n'est pas reconnu (son empreinte de référence n'est pas dans la base), l'accès est refusé.

Voir la section Contrôle d'accès par authentification.

Authentification avec empreintes de référence dans le terminal (1 versus 1)

Les empreintes digitales numérisées de l'utilisateur sont stockées dans la base de données locale du terminal.

Dans ce cas, l'identifiant est utilisé comme clé de recherche pour trouver les empreintes de l'utilisateur dans la base de données locale.

L'identifiant peut être stocké sur une carte sans contacte iCLASS®, MIFARE®, ou DESFire®.

Mode Proxy

Le mode Proxy n'est pas un mode de contrôle d'accès à proprement parlé. Dans ce mode, le terminal MorphoAccess® agit comme un esclave et attend des commandes venant de l'extérieur comme :

- Identification,
- Authentification,
- Activation du relais,
- Lecture de données sur une carte sans contact,
- …

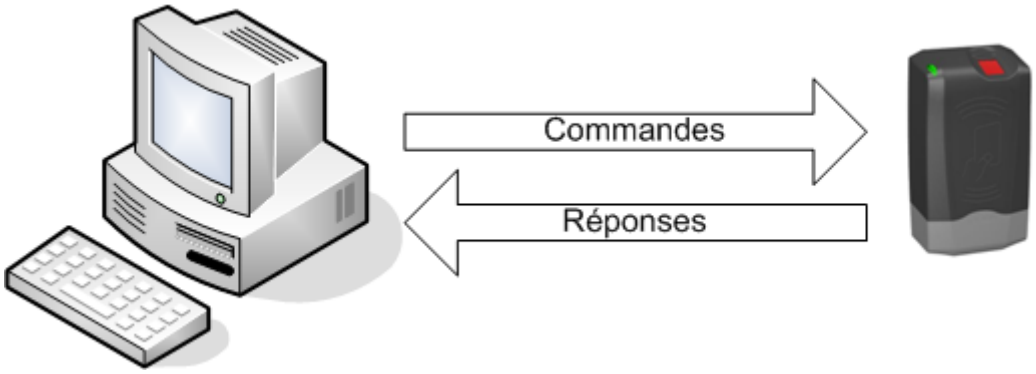


Figure 6 : Mode Proxy

Se référer au chapitre Mode PROXY pour plus de détails sur la gestion à distance.

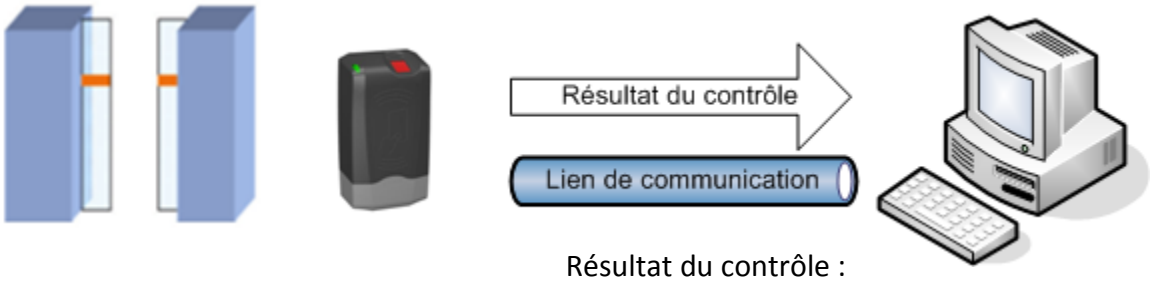
Se référer au document *MorphoAccess® Host System Interface Specification* pour la liste complète des commandes.

Communication du résultat du contrôle d'accès

Lorsque l'accès est autorisé (l'utilisateur a été reconnu), un voyant lumineux (LED) passe au vert et le terminal émet un signal aigu.

Lorsque l'accès est refusé (l'utilisateur n'a pas été reconnu), la LED passe au rouge et le terminal émet un signal grave.

Divers messages ou interfaces peuvent être activés pour communiquer le résultat du contrôle :



Résultat du contrôle :

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

Figure 7 : Envoi du résultat du contrôle d'accès local

Relais

Si configuré, et après un contrôle réussi, le relais peut être activé pendant une certaine période (ouverture d'une porte actionnée par une gâche.)

Lien Wiegand/Dataclock

Le résultat du contrôle d'accès peut être envoyé sur un lien Wiegand ou Dataclock.

Le message contient uniquement l'identifiant de l'utilisateur (qui doit être une valeur numérique). Par défaut, le résultat est seulement envoyé lorsque le contrôle est réussi, mais selon la configuration du terminal, le résultat peut aussi être envoyé en cas de refus. Dans ce cas, le message contient un code d'erreur au lieu de l'identifiant de l'utilisateur.

Lien IP

Le résultat du contrôle peut être envoyé au travers d'une connexion IP en utilisant les protocoles UDP, TCP, ou SSL.

Se référer eu document *MorphoAccess® Remote Messages Specification* pour connaître les informations envoyées par le terminal.

L'administrateur peut configurer le port et définir le protocole.

Se référer au document *Solution SSL pour MorphoAccess®*, pour plus de détails sur l'utilisation du protocole SSL.

Lien série RS485

Le résultat du contrôle peut être envoyé sur le lien Wiegand/Dataclock en utilisant le protocole RS485.

Se référer au document *MorphoAccess® Remote Message Specification* pour connaître les informations envoyées par le terminal.

Journal local (« log »)

Si configuré, le terminal crée un enregistrement pour chaque contrôle d'accès dans un fichier local. Chaque enregistrement inclut : la date et l'heure du contrôle, l'identifiant de l'utilisateur (si disponible), et le résultat du contrôle.

Le contenu de ce fichier peut être téléchargé par un hôte distant, ou exporté sur une clé USB de stockage.

Le terminal peut enregistrer jusqu'à 65000 contrôles. Quand le fichier est plein, les enregistrements ne se font plus

Se référer à la section Émission du résultat pour plus de détails.

Configuration du terminal

Ce chapitre décrit comment configurer un terminal MorphoAccess®. Les paramètres peuvent être changés à distance par le réseau.

Comprendre la configuration du MorphoAccess®

Présentation

La configuration du MorphoAccess® est stockée dans des fichiers organisés en sections et valeurs.

Par exemple, un fichier nommé « app.cfg » contient tous les paramètres caractérisant l'application principale.

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

Organisation de la configuration

Le terminal crée plusieurs fichiers :

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

Se référer au document *MorphoAccess® Parameters Guide* pour plus de détails sur ces fichiers.

Modification d'un paramètre

A distance à travers un lien IP à l'aide d'une application dédiée sur l'hôte distant.

Notation

Dans ce document, un paramètre est présenté dans le format suivant :

"Brève description"	
fichier/section/paramètre	Valeur

Par exemple, pour activer le contrôle d'accès base sur l'identification, le paramètre suivant doit être à 1 :

Contrôle d'accès par identification	
app/bio ctrl/identification	1

Configuration d'un terminal par IP

Introduction

Un PC (typiquement, un poste avec MEMS™) connecté en réseau à un MorphoAccess®, peut administrer le terminal via un jeu de commandes. Les fonctions d'exploitation à distance sont, par exemple, les suivantes :

- ajout d'empreintes numérisées dans la base locale (enregistrement),
- modification des paramètres de contrôle,
- lecture de configuration,
- suppression de base de données locale,
- suppression d'enregistrement,
- téléchargement du journal d'événements,
- mise à jour des logiciels embarqués.

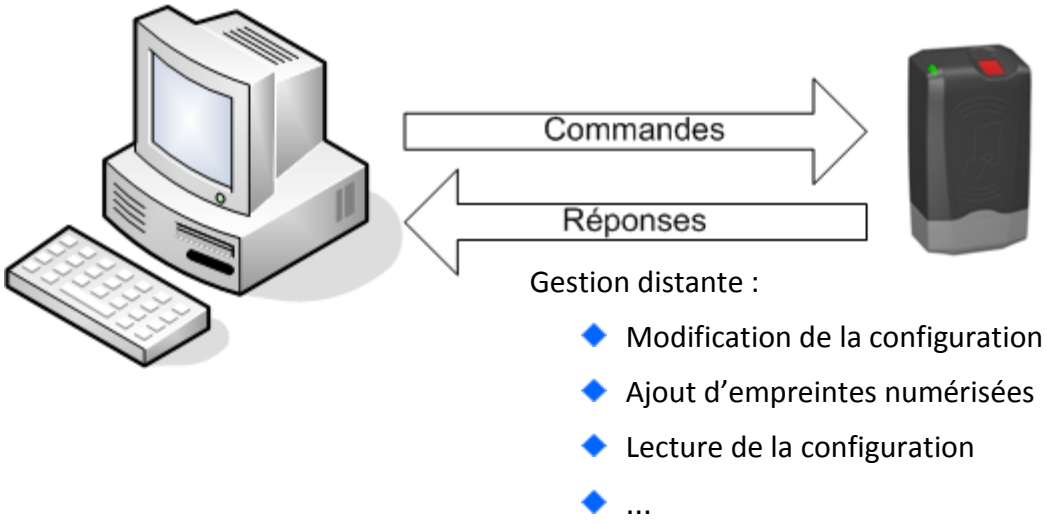


Figure 8 : Configuration du terminal par IP

Le MorphoAccess® fonctionne comme un serveur en attente d'une requête PC.

Le PC gère la base de données contenant les empreintes digitales de référence.

Veuillez vous reporter au document *MorphoAccess® Host Interface Specification* pour une description complète de la gestion à distance. Ce document explique également comment créer une base de données et sauvegarder les enregistrements biométriques dans cette base.

Paramètres usine réseau

Par défaut, l'adresse IP du terminal est *134.1.32.214*. Cette adresse peut être changée via IP ou à l'aide d'une clé USB de stockage.

Le port serveur par défaut est 11010.

Sécurisation en SSL (depuis la version 2.07 du logiciel)

La communication peut être sécurisée en SSL. Il est conseillé d'utiliser les outils proposés par Morpho (MATM avec MATM SSL Plugin).

Se référer au document *Solution SSL pour MorphoAccess®*.

"Outil de configuration"

L'outil *« Morpho Bio Toolbox »* permet de modifier la configuration d'un terminal. Ce programme est une illustration de l'utilisation des commandes ILV. Veuillez vous reporter au guide utilisateur disponible dans le menu « Aide » de l'application Morpho Bio Toolbox.

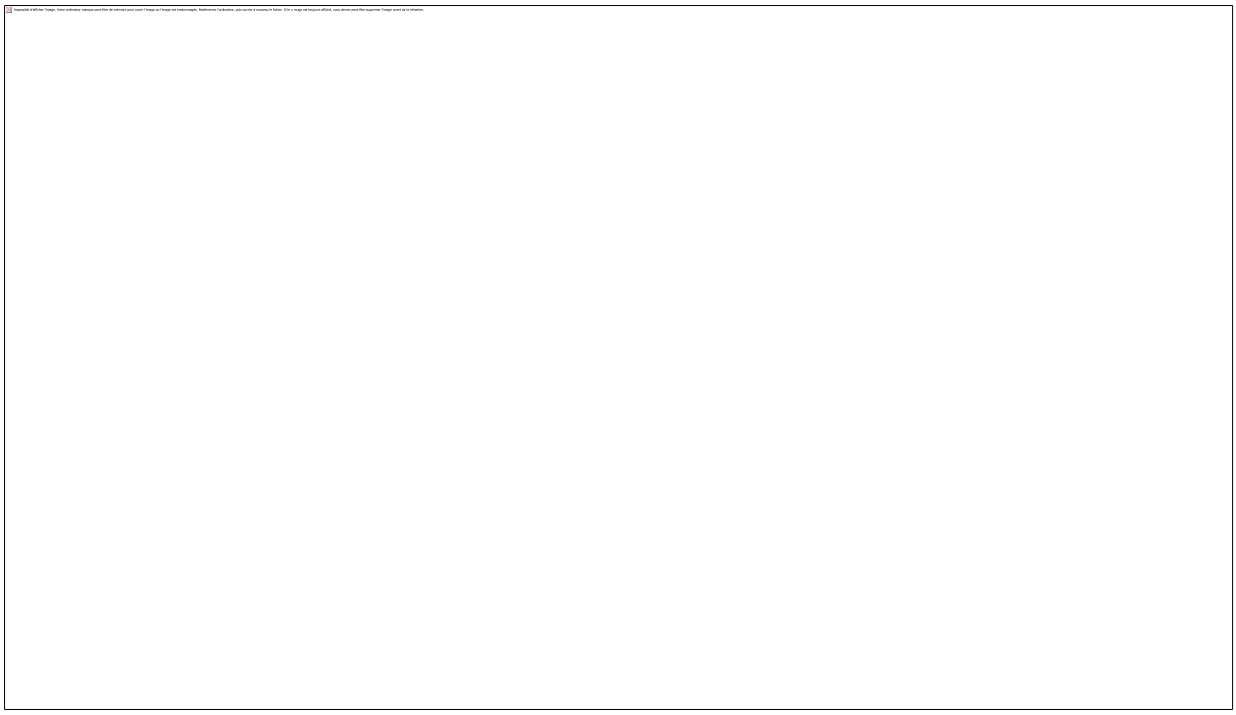


Figure 9 : Outil de configuration du terminal par IP

Mise à jour du logiciel embarqué

Il est possible de mettre à jour la version du logiciel embarqué du terminal MorphoAccess® via un lien IP.

Les versions du logiciel embarqué sont disponibles sur le CDROM ou sur le site internet de Morpho.

Veuillez utiliser l'outil *MorphoAccess QuickLoader* pour effectuer la mise à jour.

Se référer au document *MorphoAccess® Upgrade Guide* pour plus de détails sur la procédure de mise à jour du logiciel embarqué.

Configuration d'un terminal autonome

Le terminal MorphoAccess® possède deux modes de fonctionnement principaux : l'identification et l'authentification. Ces deux modes peuvent être activés simultanément (mode fusionné).

Préliminaire : Ajout d'empreintes numérisées dans le base de données locale

La gestion de la base de données biométriques d'un terminal MorphoAccess® Série 100 est effectuée par un hôte distant.

Gestion à distance

Les empreintes d'un utilisateur sont capturées sur une station d'enrôlement (un PC équipé de MEMS™ par exemple) et sont exportées sur le MorphoAccess® via un lien de communication.

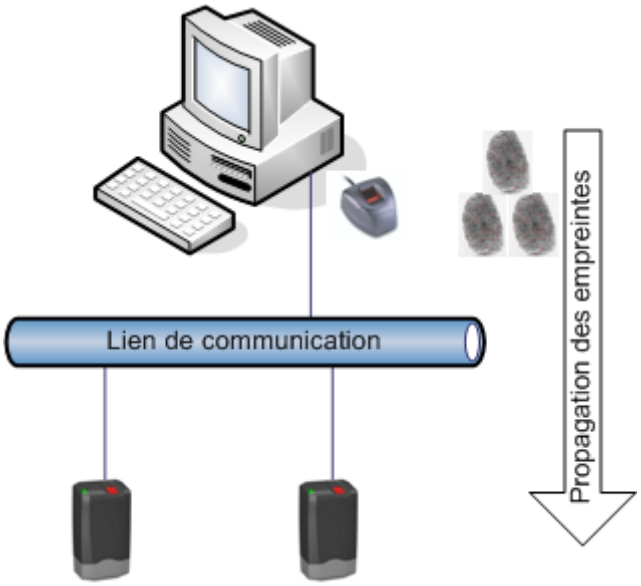


Figure 10 : Gestion à distance

Cette architecture permet la gestion de plusieurs terminaux MorphoAccess® à partir d'un seul hôte distant.

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 la valeur 1.

Dans ce mode de reconnaissance, la capteur est allumé et attend la pose d'un doigt.

Quand un doigt est présenté, l'empreinte est numérisée et comparée avec les empreintes de la base.

Si l'identification est positive, le terminal autorise l'accès ou renvoie l'ID correspondant au contrôleur de sécurité central, selon sa configuration. Un relais peut également être activé.

Lorsque l'identification de la personne est effectuée, le terminal revient automatiquement en attente d'une nouvelle empreinte.

Au moins une empreinte doit être mémorisée dans la base de données locale. Le terminal peut contenir 500 utilisateurs avec 2 empreintes chacun.

Lorsque le terminal fonctionne en mode identification avec une base de données vide, le capteur est éteint et la LED clignote en jaune.

Désactivation

Affectez à *app/bio ctrl/identification* la valeur 0 pour désactiver le mode identification.

Introduction à l'authentification par cartes sans contact

Activation de la lecture de cartes sans contact

Sur les terminaux équipés d'un lecteur de cartes sans contact (voir Objet du document), la lecture de cartes iCLASS®/MIFARE®/DESFire® peut être configurée.

Cas des MorphoAccess® équipés d'un lecteur sans contact DESFire®

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

Les terminaux MorphoAccess® 120D 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 lecture

Diverses stratégies de reconnaissance peuvent être appliquées selon l'emplacement des fichiers d'empreintes biométriques (empreintes de référence ou modèle) et le niveau de sécurité requis.

Utiliser des cartes sans contacts DESFire® suppose que l'utilisateur présente une carte DESFire® contenant des données structures (identifiant, empreintes biométriques, …).

Utiliser des cartes sans contacts MIFARE® suppose que l'utilisateur présente une carte MIFARE® contenant des données structures (identifiant, empreintes biométriques, …). Les données sont situées sur la carte par un bloc (paramètre « B ») et sont protégées par une clé (paramètre « C »). Le paramètre « C » définit quelle clé de sécurité est utilisée pendant la lecture de la carte.

Utiliser des cartes sans contacts iCLASS® suppose que l'utilisateur présente une carte iCLASS® contenant des données structures (identifiant, empreintes biométriques, …).

Pour une description complète de la structure des cartes, veuillez vous référer au document *MorphoAccess® Contactless Card Specification*.

Les modes de lectures disponibles sont les suivants :

Authentification sans contact avec empreintes de référence sur la carte :

Les empreintes relevées sont comparées aux empreintes de référence *lues sur la carte (PK)*. L'**identifiant** et les **empreintes** doivent être présents sur la carte.

Authentification sans contact avec empreintes de référence dans la base de données locale:

Les empreintes relevées sont comparées aux empreintes de référence *lues* dans la base de données locale. Seul **l'identifiant** doit être présent sur la carte.

Authentification sans contact selon le mode de la carte :

Selon le mode de la carte, soit les empreintes de référence sont lues sur la carte soit le contrôle peut être désactivé (mode visiteur). Le TAG « **mode de la carte** » doit être présent sur la carte.

Authentification - empreintes biométriques sur carte

Authentification sans contact avec empreintes numérisées (PK) sur carte	
app/bio ctrl/authent PK contactless	1

Dans ce mode, l'utilisateur présente sa carte DESFire®, MIFARE® ou iCLASS® (selon les terminaux), le terminal lit les empreintes numérisées (PK) sur la carte et procède au contrôle.

Dans ce cas, la carte contient l'identifiant utilisateur et les empreintes numérisées. Aucune base de données locale n'est nécessaire.

Si la carte contient les empreintes numérisées et l'identifiant 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.

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

Données requises sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent PK contactless	Oui	Non	Oui	Oui	Non	Non

La structure des données enregistrées sur les cartes sans contact est décrite dans *MorphoAccess® Contactless Card Specification*.

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 à un endroit précis de la carte (ID binaire).

ID codé en ASCII, données structurées

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

L'identifiant doit être enregistré dans une structure TLV.

Identifiant ASCII, données structurées par une suite de « tags »	
app/contactless/data format	0
app/contactless/data length	0
app/contactless/data offset	0

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

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

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.

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	
app/bio ctrl/authent ID contactless	1

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

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

Identifiant binaire	
app/contactless/data format	1

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.

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	
app/contactless/B	[1-215] : bloc de lecture
app/contactless/data length	[nombre d'octets].[nombre de bits]
app/contactless/data offset	[nombre d'octets].[nombre de bits]

La manière dont l'identifiant sera interprété est configurable.

Interprétation des données	
app/contactless/data type	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 référence associées à cet identifiant sont utilisées lors de l'authentification.

Le déroulement de l'authentification est identique à celui décrit précédemment.

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).

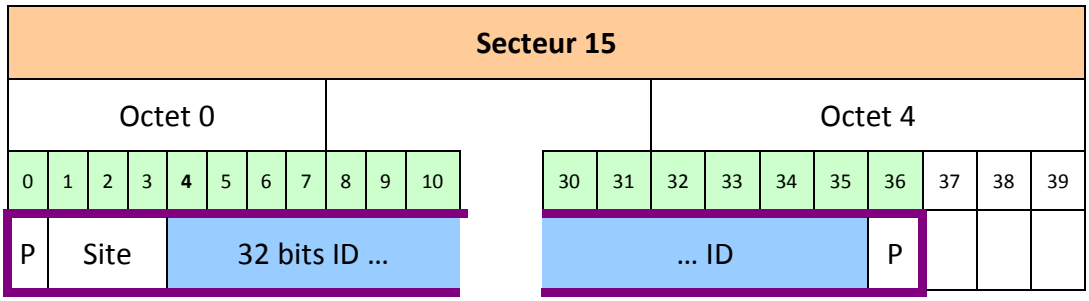
Exemple – lecture du Numéro de Série de la carte MIFARE® (format little endian).

- 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 :

app/contactless/data format = 1	ID binaire
app/contactless/data type = 0.1	ID binaire en MSB
app/contactless/data length = 4.0	ID de 4 octets
*app/contactless/data offset = 0.**4***	ID au 4ème bit du secteur 15.
app/contactless/B = 46	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

Authentification sans contact selon le mode de la carte	
app/bio ctrl/authent card mode	1

Dans ce mode, la carte « décide » du déroulement du contrôle.

La donnée « CARD MODE » est requise. On peut lui attribuer deux valeurs :

- PKS [0x02] : l'identifiant et les deux empreintes de l'utilisateur sont également requis sur la carte. L'authentification biométrique s'effectue par rapport aux empreintes de référence lues sur la carte,
- ID_ONLY [0x01] : seul l'identifiant de l'utilisateur est également nécessaire. Il n'y a pas de contrôle biométrique, le contrôle est immédiatement positif. Cette fonction est utile pour un visiteur nécessitant un accès sans enregistrement.

Pour activer ce mode, affectez à *app/bio ctrl/authent card mode* la valeur 1.

Pour désactiver ce mode, affectez à *app/bio ctrl/authent card mode* la valeur 0.

Données requises sur la carte

Si la valeur de la donnée CARD MODE est ID_ONLY.

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

Si la valeur de la donnée CARD MODE est PKS.

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

La structure de la carte est décrite dans *MorphoAccess® 100 Series Contactless Card Specification*.

Note à propos de la désactivation du contrôle biométrique :

Lorsque la désactivation du contrôle biométrique est activée par la configuration du terminal (voir Désactiver le contrôle biométrique dans l'authentification), le mode d'authentification imposée par la carte est ignoré.

Mode « multi-facteur » ou fusionné

Ce mode est la fusion du mode identification et du mode authentification sans contact et sans base de données.

Ce mode permet donc de :

- lancer une identification lorsque l'utilisateur positionne son doigt (fonctionnement identique au mode identification),
- lancer une authentification sans contact lorsque l'utilisateur place sa carte sans contact (fonctionnement identique à l'authentification sans mode base de données).

En l'absence de base de données, la présentation de badges sans contact reste possible.

Ce mode est activé en activant un mode d'authentification sans contact et l'identification.

Mode fusionné	
app/bio ctrl/identification	1
Et	
app/bio ctrl/authent PK contactless	0 ou 1
app/bio ctrl/authent card mode	0 ou 1
app/bio ctrl/authent ID contactless	0 ou 1

Les données requises sur la carte dépendent du mode d'authentification, mais au moins la donnée identifiant est obligatoire.

Désactiver le contrôle biométrique dans l'authentification

Dans ce mode, seul l'identifiant de l'utilisateur est requis sur la carte. Ce mode doit être combiné avec un mode d'authentification. L'activation de ce mode signifie que la vérification biométrique n'est pas effectuée.

Le terminal vérifie la présence de l'identifiant dans la base locale

Combiné avec le mode « *authent ID contactless* », le MorphoAccess® vérifie que l'identifiant lu sur la carte est présent dans la base de données locale avant d'accorder l'accès.

Désactivation du contrôle biométrique, mais ID doit être présent dans la base de données locale	
app/bio ctrl/bypass authentication	**1**
app/bio ctrl/authent ID contactless	1

Données requises sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non

Le terminal fonctionne comme un simple lecteur sans contact

Combiné avec le mode « *authent PK contactless* », le MorphoAccess® autorise toujours l'accès : le terminal fonctionne comme un simple lecteur de carte DESFire®, MIFARE® ou iCLASS®.

Désactivation du contrôle biométrique, l'accès est toujours accordé.	
app/bio ctrl/bypass authentication	**1**
app/bio ctrl/authent PK contactless	1

Pour désactiver le contrôle biométrique, attribuez à *app/bio ctrl/bypass authentication* la valeur 1.

Pour activer le contrôle biométrique, attribuez à *app/bio ctrl/bypass authentication* la valeur 0.

Données requises sur la carte

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non

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

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

Désactivation du contrôle biométrique, l'accès est toujours accordé	
app/bio ctrl/bypass authentication	**1 *(Enabled)***
app/bio ctrl/authent PK contactless	1 *(Enabled)*
app/bio ctrl/authent ID contactless	1 *(Enabled)*

Données binaires	
app/contactless/data format	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 V2.09.

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, l'accès est toujours accordé, activation d'un mode sans contact	
app/bio ctrl/bypass authentication	**1 *(Activé)***
app/bio ctrl/authent PK contactless	1 *(Activé)*
app/bio ctrl/authent ID contactless	1 *(Activé)*

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

Synthèse des modes de reconnaissance

Le mode de reconnaissance repose sur les éléments suivants :

- le mode d'authentification ou d'identification requis : Carte seule, Carte + Biométrie, Biométrie seule,
- ce qui définit le mode d'exploitation : la carte ou le terminal.

	Mode défini par la Carte *app/bio ctrl/authent card mode* *1*	**Mode défini par le terminal** *app/bio ctrl/authent card mode* *0*
Mode opératoire		
Authentification de la carte MorphoAccess® avec lecteur de cartes	**ID dans la carte** Card Mode Tag = ID_ONLY	**ID dans la carte** bypass authentication 1 authent ID contactless 1 ***Vérification de l'ID dans le terminal.***
		ID dans la carte bypass authentication 1 authent PK contactless 1 ***Pas de vérification de l'ID dans le terminal.***
Authentification de la carte et des données biométriques MorphoAccess® avec lecteur de cartes	**ID et données BIO dans la carte** Card Mode Tag = PKS	**ID et données BIO dans la carte** bypass authentication 0 authent PK contactless 1
		ID dans la carte et données BIO dans le terminal bypass authentication 0 authent ID contactless 1
Identification des données biométriques Tout MorphoAccess®		**ID et données BIO dans le terminal** identification 1

Définition du mode de reconnaissance

Mode « 2 tentatives »

Si la reconnaissance échoue, on peut donner une 2ème chance à l'utilisateur.

En mode identification, si un doigt est mal reconnu, l'utilisateur a 5 secondes pour représenter une seconde fois le doigt. Le résultat est envoyé suite à une deuxième présentation du doigt ou à la fin de ce délai.

En mode authentification, si un doigt est mal reconnu, une deuxième tentative est possible sans avoir à représenter le badge. Le résultat est envoyé seulement après la seconde tentative.

Il est possible de paramétrer le temps de présentation de doigt et de désactiver ce mode « 2 tentatives ».

La deuxième tentative utilise un mode de reconnaissance affiné mais plus lent.

Paramètres

Ce mode peut être configuré à partir de l'outil *Morpho Bio Toolbox* par exemple.

Par défaut le mode « 2 tentatives » est activé :

Activation du nombre de tentatives	
app/bio ctrl/nb attempts	1 (seulement 1 tentative) 2 (mode « 2 tentatives »)

En mode identification (mode « 2 tentatives »), le temps maximal d'attente d'un doigt à la seconde tentative peut être configuré :

Configuration du temps d'identification	
app/bio ctrl/identification timeout	5 (1-60)

En mode authentification, le temps pour présenter un doigt à chaque tentative peut être configuré :

Configuration du temps d'authentification	
app/bio ctrl/authent timeout	(1-60)

Définition des paramètres de reconnaissance

Définition du seuil de reconnaissance	
bio/bio ctrl/matching th	1-10

Les performances d'un système biométrique sont caractérisées par deux grandeurs : le taux de rejet (FRR) et le taux de fausse acceptante (FAR).

Différents compromis sont possibles entre le taux de rejet et le taux de fausse acceptance, 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 acceptance 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 prendre une valeur comprise entre 1 et 10. Il indique le degré du seuil de reconnaissance. Les valeurs de définition du seuil sont identifiées ci-dessous.

1	Très peu de personnes sont rejetées	FAR < 1%
2		FAR < 0.3%
3	Valeur recommandée (valeur par défaut)	FAR < 0.1%
4		FAR < 0.03%
5	Seuil intermédiaire	FAR < 0.01%
6		FAR < 0.001%
7		FAR < 0.0001%
8		FAR < 0.00001%
9	Seuil très élevé (peu de fausses acceptances). Application de haute sécurité.	FAR < 0.0000001%
10	Seuil élevé pour objet de test seulement	Il y a très peu de fausses reconnaissances et beaucoup de rejets.

Mode proxy

Présentation du mode Proxy

This operating mode allows controlling the MorphoAccess® remotely using a set of biometric and databases management commands.

In Proxy mode the access control is performed remotely by the Host System: the MorphoAccess® works as a slave waiting for external commands such as:

Ce mode permet de commander le MorphoAccess® à distance à l'aide d'un jeu de commande.

En mode Proxy, le contrôle d'accès est effectué par l'intermédiaire d'un hôte distant. Le terminal fonctionne en esclave et attend des commandes telles que :

- identification de l'utilisateur,
- authentification de l'utilisateur,
- ouverture du relais,
- lecture d'une carte sans contact,
- gestion des données biométriques,
- gestion de la configuration du terminal,
- …

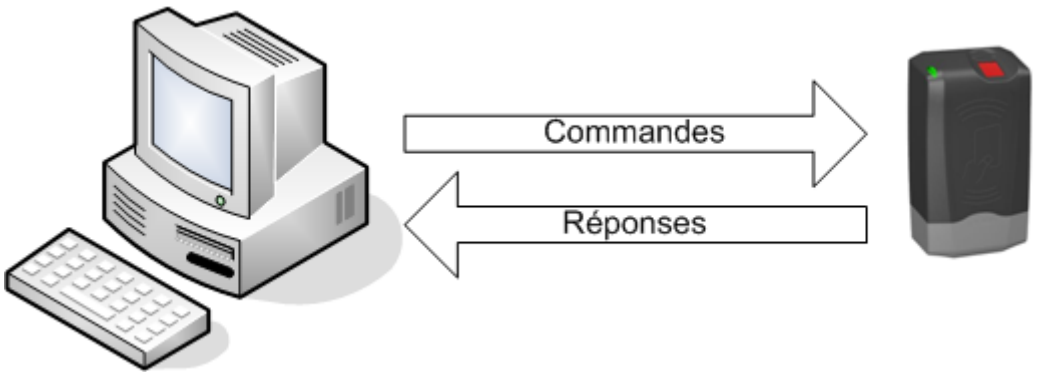


Figure 11 : Mode Proxy

Veuillez vous référer au document *MorphoAccess® Host System Interface Specification*: ce document détaille comment gérer un MorphoAccess® à distance.

Activation du mode Proxy

L'identification et l'authentification doivent être désactivées. Cela signifie que tout contrôle doit être désactivé. Le terminal devient esclave.

Mode Proxy	
app/bio ctrl/identification	**0**
app/bio ctrl/authent PK contactless	**0**
app/bio ctrl/authent ID contactless	**0**
app/bio ctrl/authent card mode	**0**

Personnalisation du terminal MorphoAccess®

Contrôle horaire

En utilisant MEMS™, la fonctionnalité de contrôle horaire est disponible. Cette fonctionnalité permet de contrôler les plages horaires d'accès avant d'autoriser ou non l'accès. Les plages horaires sont définies par plages de 15 minutes pour une semaine complète.

Activation du contrôle horaire	
app/modes/time mask	1 *(Enabled)*

Pour utiliser cette fonctionnalité, la base de données locale doit avoir été créée avec un champ additionnel particulier. Si ce champ additionnel n'est pas présent, l'utilisation de cette fonctionnalité entraînera le refus d'accès pour tous les utilisateurs.

Veuillez vous référer au document *MorphoAccess® Host Interface Specification* pour savoir comment créer une base de données compatible avec le contrôle horaire.

Compatibilité avec un système de contrôle d'accès

Envoi de l'identifiant vers le contrôleur central

Présentation

Le MorphoAccess® peut envoyer des messages d'état en temps réel à un contrôleur par divers moyens et via plusieurs protocoles. Ces informations peuvent être utilisées, par exemple, pour afficher sur un écran externe le résultat d'une opération biométrique, le nom ou l'ID de la personne identifiée, selon le rôle du contrôleur dans le système.

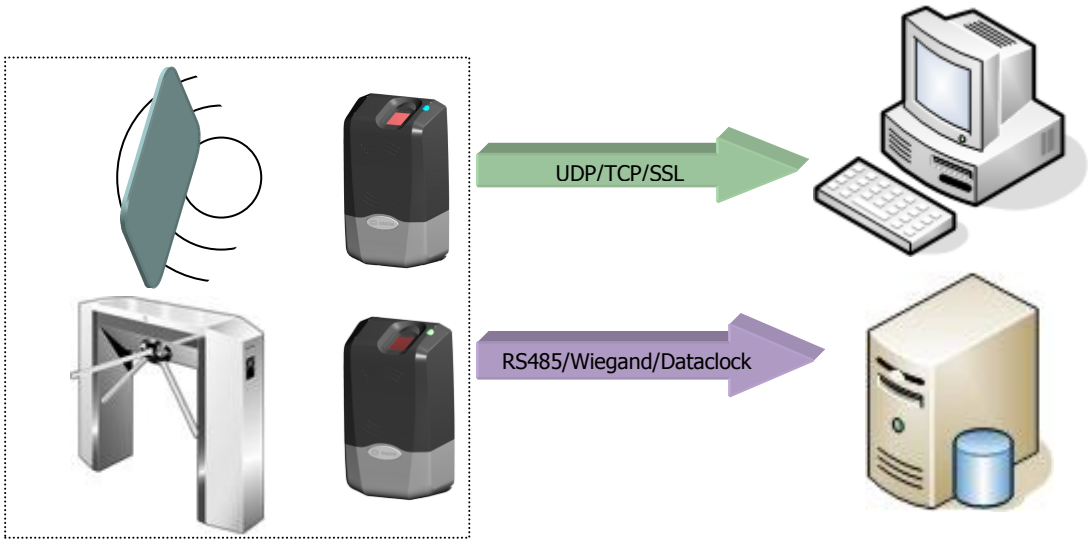


Figure 12 : Envoi du résultat du contrôle d'accès local

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

Protocoles pris en charge

Le terminal peut envoyer des messages sur les opérations biométriques effectuées par le MorphoAccess® à un contrôleur via les interfaces suivantes :

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

Veuillez vous référer au document *Solution SSL pour MorphoAccess®* pour plus d'information sur l'utilisation du SSL.

Utilisation du relais

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

Activation du relais	
app/relay/enabled	1

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	
app/relay/aperture time in 10 ms	300 (50 à 60 000)

L'état de repos du relais peut être défini.

État de repos du relais	
app/relay/relay default state	0 (par défaut) 1

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

Commande déportée du relais

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.

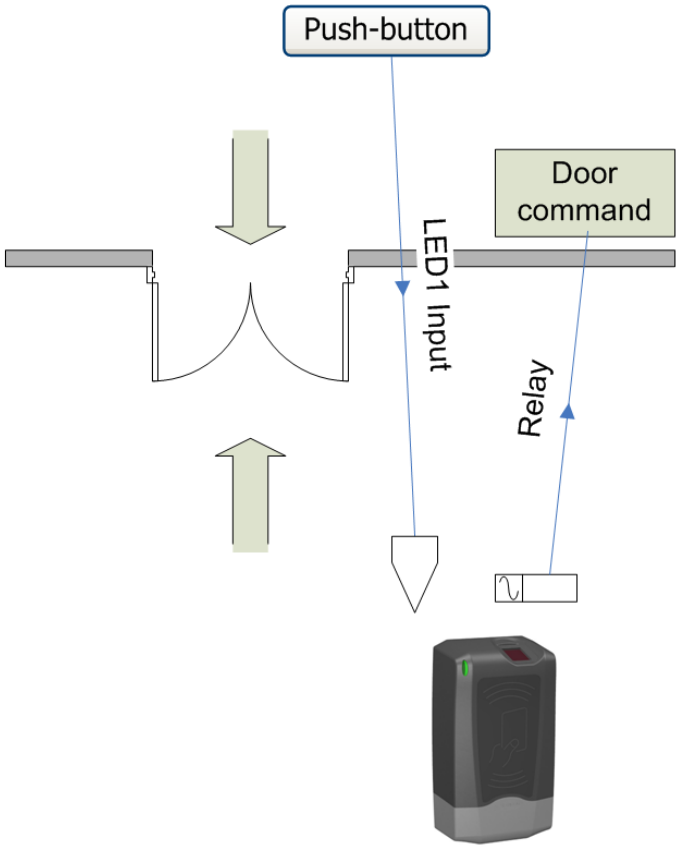


Figure 13 : Pilotage du relais interne par signal LED1

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.

Journal interne

Le MorphoAccess® consigne ses activités	
app/log file/enabled	1

Le MorphoAccess® peut consigner ses activités biométriques. Il enregistre le résultat du contrôle, la date et l'heure, l'heure d'exécution et l'ID de l'utilisateur.

Le terminal MorphoAccess® est capable de gérer jusqu'à 65000 enregistrements.

Il est possible de télécharger le fichier journal. Pour plus d'informations sur cette fonction, voir *MorphoAccess® Host System Interface*.

Activation d'actions particulières lorsque le fichier est plein	
app/log file/full handling	"00000000" (no specific action)

Selon sa configuration, lorsque la limite du journal est atteinte, le terminal MorphoAccess® peut effectuer les actions suivantes :

- Envoyer un message d'information à un hôte distant (cf.)
- Effacer le fichier d'enregistrements.

Pour plus de détails, se référer au document *MorphoAccess® Parameters Guide*.

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 ».

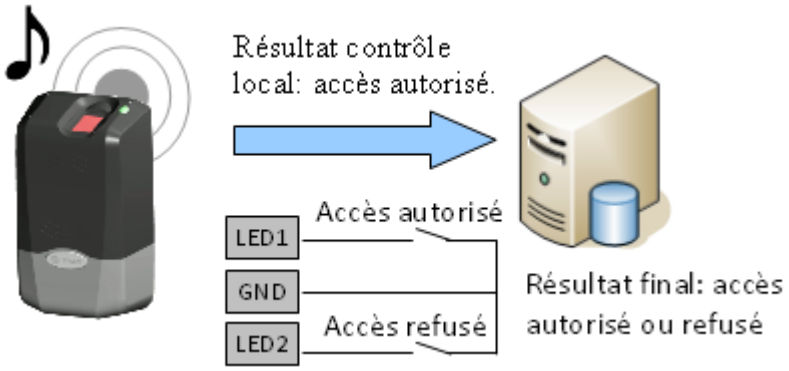


Figure 14 : Fonctionnalité LED IN

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)

Sécurité du terminal

Gestion du switch anti intrusion

Activation de l'alarme

En cas d'intrusion (ouverture du capot inférieur), le terminal peut envoyer un message d'alarme au travers des protocoles décrits ci-dessus. Il peut également émettre une alarme sonore en parallèle de l'envoi de message.

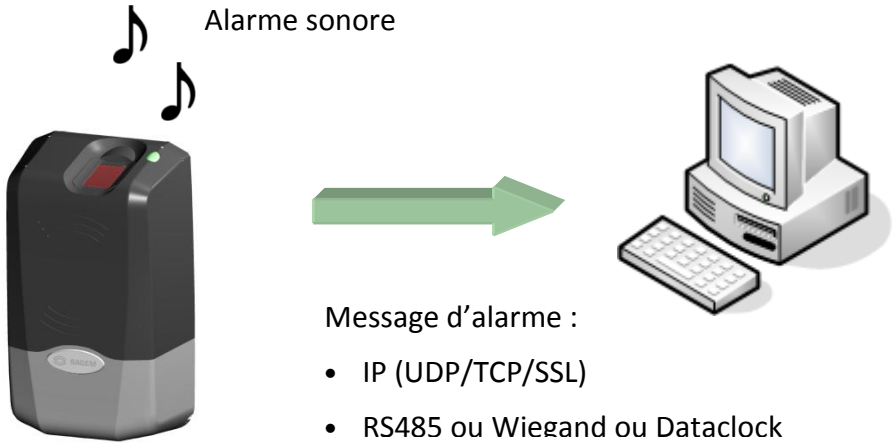


Figure 15 : Gestion intrusion

Pour envoyer un message en cas d'intrusion (IP, RS485, Wiegand, DataClock), l'interface correspondante doit être activée.

Comme le RS485, le Wiegand et le Dataclock partagent la même interface physique, seulement un seul de ces protocoles doit être activé, autrement la priorité est donnée au Wiegand, puis Dataclock et RS485.

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 (sélection du lien RS485),
- app/send ID UDP/enabled,
- app/send ID ethernet/mode (choix entre UDP ou TCP),
- app/send ID ethernet/SSL *enabled (se référer au document* Solution SSL pour MorphoAccess®*).*

Le système de gestion de l'alarme anti-intrusion peut être configuré en validant la clé *app/tamper alarm/level* avec la valeur appropriée.

Indications de l'alarme anti-intrusion	
app/tamper alarm/level	0-2
0 Pas d'alarme.	
1 Alarme par message (Pas d'alarme sonore).	
2 Alarme par message et sonore (buzzer)	

La clé *app/failure ID/Alarm ID* définit la valeur de l'identifiant d'alarme à envoyer sur Wiegand ou Dataclock. Cet identifiant permet de se distinguer des autres : identifiant utilisateurs et identifiant de pannes. La clé *app/failure ID/enabled* doit être validée afin d'activer l'envoi de l'identifiant d'alarme.

Identifiant de l'alarme anti-intrusion	
app/failure ID/alarm ID	0- 65535
app/failure ID/enabled	1

En Wiegand et en Dataclock, l'ID d'alarme est envoyé comme les ID d'erreurs. Voir la documentation *MorphoAccess® Remote Messages Specification* pour la description du format des paquets UDP et RS485.

Exemples

Exemple 1: Envoi d'un ID alarme (62221) en Wiegand, et avertissement sonore, en cas de détection d'intrusion

Pour envoyer une alarme en Wiegand, la clé *app/send ID wiegand/enabled* doit être mise à 1, et la clé *app/tamper alarm/level* doit être mise à 2 (alarme et buzzer).

La clé *app/failure ID/alarm ID* doit être mise à 62221 pour identifier l'événement d'alarme.

Exemple 2: Envoi d'une alarme d'intrusion en UDP.

Pour envoyer une alarme en UDP, la clé *app/send ID UDP/enabled* doit être mise à 1.

La clé *app/tamper alarm/level* doit être mise à 1 (alarme silencieuse).

Envoi de messages

Cette section décrit la façon dont les terminaux MorphoAccess® Série 100 peuvent envoyer des messages à une tierce entité. Ces messages ne sont pas équivalents aux messages d'envoi de résultats.

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 interne plein

Veuillez vous référer au document *MorphoAccess® Remote Message 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	
Events/general/active	"FFFFFFFF" (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"	
Events/log_full/nb sending	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).

Veuillez 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	
Remotemsg/interface/nb interfaces	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

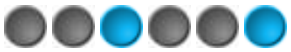
Veuillez vous référer au document *MorphoAccess® Parameters Guide* pour plus de détails concernant la configuration des interfaces.

Interface « homme – machine »

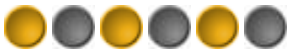
Convention

Signaux lumineux

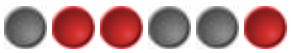
La LED émet un signal très bref sur une période assez lente.

Signal bref 

La fréquence de clignotement est élevée. On peut comparer ce signal à l'activité d'un disque dur.

« Fréquence élevée » 

Cas d'un clignotement « lent. » La fréquence de clignotement de la LED est d'une seconde environ.

« Fréquence faible » 

Signal sonore

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

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

Etat du terminal

Identification – attente de la présentation d'un doigt

Capteur	ON
LED	OFF

Authentification – attente d'un badge sans contact

Capteur	OFF
LED	Signal bref

Fusion – attente d'un doigt ou d'un badge

Capteur	ON
LED	Signal bref

Absence de base de données ou base de données vide

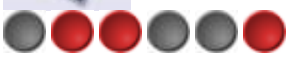
Capteur	OFF
LED	« Fréquence faible »

Acquisition biométrique, mauvais positionnement

Capteur	ON
LED	« Fréquence élevée »

Capteur biométrique en défaut

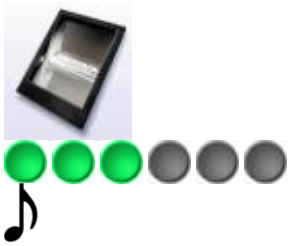
Capteur	OFF
LED	« Fréquence faible »



Résultat du contrôle de droits d'accès

Contrôle OK

Capteur	ON
LED	Verte 1 seconde
Buzzer	ON 0,1 seconde – tonalité aiguë



Échec du contrôle

Capteur	ON
LED	Rouge 1 seconde
Buzzer	ON 0,7 seconde – tonalité grave

Maintenance

La clé USB peut être retirée

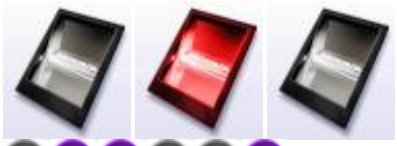
Capteur	-	-
LED	« Fréquence élevée »	
Buzzer	ON 0,7 seconde – tonalité grave	

Administration à distance

Une opération d'administration est en cours. Il peut s'agir par exemple d'une mise à jour de la base de données.

Capteur	OFF	
LED	« Fréquence faible »	

Le logiciel embarqué du capteur biométrique est en cours de mise à jour.

Capteur	Clignotement rapide.	
LED	« Fréquence faible »	

Annexes

Compatibilité MorphoAccess® 220/320

Ces tables présentent l'équivalence de paramètres entre la famille MorphoAccess® 320/220 et la famille MorphoAccess® 120.

Mode fusionné (*/cfg/Maccess/Admin/mode 5* sur MA220 et MA320) activé lorsque la valeur 1 est attribuée à *app/bio ctrl/identification*.

MA220/320	MA120 et MA120 D
Authentification sans contact avec ID sur la carte, empreintes numérisées dans la base de données locale	
/cfg/Maccess/Admin/mode 4	*app/bio ctrl/authent ID contactless 1*
Authentification sans contact, mode défini par la carte	
/cfg/Maccess/Contactless/without DB mode 0 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent card mode 1*
/cfg/Maccess/Admin/mode 5 *(mode fusionné)*	*app/bio ctrl/identification 1*
Authentification sans contact, vérification biométrique par rapport aux empreintes contenues dans la carte	
/cfg/Maccess/Contactless/without DB mode 2 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent PK contactless 1*
/cfg/Maccess/Admin/mode 5 *(mode fusionné)*	*app/bio ctrl/identification 1*
Authentification sans contact : ID seulement, pas de vérification biométrique	
/cfg/Maccess/Contactless/without DB mode 1 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent PK contactless 1* *app/bio ctrl/bypass authentication 1*
/cfg/Maccess/Admin/mode 5 *(mode fusionné)*	*app/bio ctrl/identification 1*

Table ModeS Sans Contact

Opération	*Mode carte authentification*	*PK authentification sans contact*	*ID authentification sans contact*	*Outrepasser l'authentification*
Authentification avec empreintes de référence dans la base de données - Lecture de l'ID sur la carte sans contact. - Récupération des empreintes de référence associées à cet ID dans la base de données. - Authentification biométrique par rapport à ces empreintes de référence. - Si l'authentification est positive, envoi de l'ID.	0	0	1	0
Authentification avec empreintes sur la carte - Lecture de l'ID et des empreintes sur la carte sans contact. - Authentification biométrique par rapport à ces empreintes. - Si l'authentification est positive, envoi de l'ID.	0	1	0	0
Authentification mode carte - Lecture du mode de fonctionnement de la carte, de l'ID, et s'ils sont requis par le mode de fonctionnement de la carte, lecture des empreintes sur la carte sans contact. - Si le mode de fonctionnement de la carte est « ID seul », envoi de l'ID. - Si le mode de fonctionnement de la carte est « Authentification avec empreintes sur la carte », authentification biométrique par rapport aux templates lus sur la carte, puis si l'authentification est positive, envoi de l'ID.	1	0	0	0
Authentification avec empreintes dans la base de données – contrôle biométrique désactivé - Lecture de l'ID sur la carte sans contact. - Vérification de la présence des empreintes associées	0	0	1	1

à cet ID dans la base de données. - Si les empreintes sont présentes, envoi de l'ID.				

Opération	*Mode carte authentification*	*PK authentification sans contact*	*ID authentification sans contact*	*Outrepasser l'authentification*
Authentification avec empreintes sur la carte – contrôle biométrique désactivé - Lecture de l'ID. - Envoi de l'ID.	**0**	**1**	**0**	**1**
Authentification mode carte – contrôle biométrique désactivé - Lecture du mode de fonctionnement de la carte, de l'ID, et s'ils sont requis par le mode de fonctionnement de la carte, lecture des templates sur la carte sans contact. - Quel que soit le mode de fonctionnement de la carte, envoi de l'ID.	**1**	**0**	**0**	**1**

« TAG » requis sur 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 empreintes sur la carte	Oui	Non	Oui	Oui	Non	Non
Authentification mode carte (ID_ONLY)	Oui	Oui	Non	Non	Non	Non
Authentification mode carte (PKS)	Oui	Oui	Oui	Oui	Non	Non
Authentification avec empreintes dans la base de données – contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non
Authentification avec empreintes sur la carte – contrôle biométrique désactivé	Oui	Non	Non	Non	Non	Non
Authentification mode carte (ID_ONLY) – contrôle biométrique désactivé	Oui	Oui	Non	Non	Non	Non
Authentification mode carte (PKS) – contrôle biométrique désactivé	Oui	Oui	Oui	Oui	Non	Non

Bibliographie

Informations à l'attention de l'administrateur

MorphoAccess® Série 100 Manuel Utilisateur

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

MorphoAccess® Parameters Guide

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

Solution SSL pour MorphoAccess®

Ce document décrit les outils et procédure pour la sécurisation en SSL des communications.

Informations à l'attention de l'installateur

MorphoAccess® Série 100 Manuel d'Installation

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

MorphoAccess® USB Network Tool User Guide

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

MorphoAccess® Upgrade Guide

Présentation des outils et des procédures de mise à jour des logiciels embarqués.

Support

FAQ

Adresse IP terminal inconnue ou terminal non joignable

Utilisez une clé USB et l'outil *USB_Network_Tool* pour définir une adresse réseau valide dans votre terminal.

Capteur est éteint

Vérifier que la base contient au moins un enregistrement.

Vérifier que le mode identification est activé.

Le terminal renvoie des réponses aléatoires aux requêtes Ping

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

Contacts

Service client

Morpho

SAV Terminaux Biométriques

Boulevard Lénine - BP428

76805 Saint Etienne du Rouvray

FRANCE

Tél: 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 01 58 11 39 19

(de 9H00 à 17H00 heure française, du Lundi au Vendredi)

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

L'accès aux parties privées du site nécessite un nom d'utilisateur (login) et un mot de passe (password).

Veuillez nous contacter afin d'obtenir votre login et mot de passe, de préférence par messagerie plutôt que par téléphone.

http://www.morpho.com/

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