

VisionPass

Guide d'Utilisation Rapide



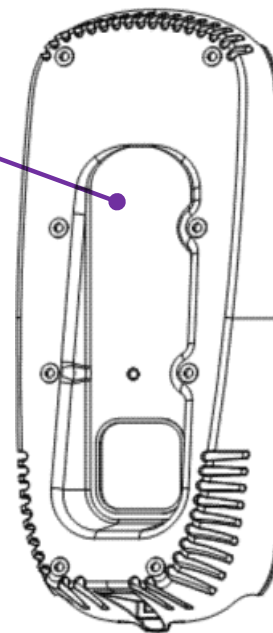
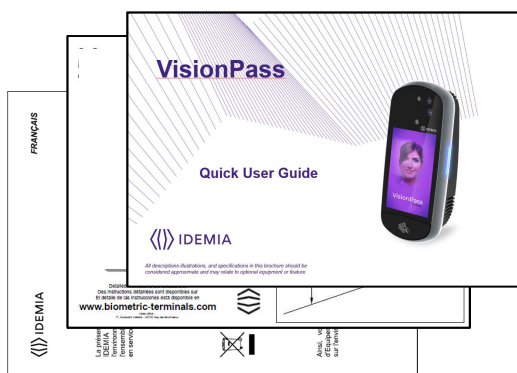
Toutes les descriptions, illustrations et spécifications contenues dans cette brochure doivent être considérées comme approximatives et peuvent concerner des équipements ou des caractéristiques optionnels



VisionPass : contenu de l'emballage

Vérification du contenu de l'emballage du terminal :

QTE	ARTICLE
1	Terminal VisionPass
1	Plaque de fixation au mur
1	Documentation



La documentation électronique est fournie au format Adobe® Acrobat® (PDF). Le lecteur Adobe® Acrobat® est disponible sur le site <http://www.adobe.com>.



Regulatory, safety and environmental notices



Les produits portant le marquage CE sont conformes à une ou plusieurs des directives européennes suivantes, selon le cas :

- Directive sur les équipements radio (Rouge) 2014/53/UE
- Directive RoHS 2011/65/UE.

La conformité à ces directives est évaluée à l'aide des normes européennes harmonisées applicables.



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

Il est fortement recommandé d'utiliser une alimentation électrique de classe II à 12V-24V et 3 A min (à 12V) en conformité avec la norme TBTS (Très Basse Tension de Sécurité). La longueur du câble d'alimentation en courant alternatif ne doit pas dépasser 10 mètres.

Ce système doit être installé conformément au Code national de l'électricité (NFPA 70), et à l'autorité locale compétente.

Ce produit est destiné à être installé avec une alimentation électrique conforme à la norme IEC 60950-1 ou IEC 62368-1, en accord avec les exigences NEC Classe 2 ; ou fournie par alimentation externe IEC 60950-1 ou IEC 62368-1 marquée Classe 2, source à puissance limitée, ou LPS et d'une puissance nominale de 12VDC, 3 A minimum ou 24VDC, 1,5 A minimum.

En cas de connexion entre bâtiments, il est recommandé de brancher le 0V à la terre. Le câble de terre doit être connecté au bornier Power Ground.

Notez que toutes les connexions de la borne VisionPass décrites ci-après sont de type TBTS (Très Basse Tension de Sécurité).



Ce symbole signifie que vous ne devez pas jeter votre produit avec vos autres déchets ménagers. Vous devez protéger la santé humaine et l'environnement en remettant vos équipements usagés à un point de collecte désigné pour le recyclage des déchets d'équipements électriques et électroniques.

Ce produit est classé comme produit laser de classe 1 selon la norme IEC 60825-1 : 2014



Table des matières

Couleur	Chapitre	Contenu
	Un	Présentation générale
	Deux	Câblage
	Trois	Communication
	Quatre	ACP ou SDAC
	Cinq	Administration
	Six	Logiciel
	Sept	Enrôlement
	Huit	Fonctions disponibles en option



Présentation générale du produit

VisionPass fournit une solution innovante et efficace pour les applications de contrôle d'accès utilisant des acquisitions très rapides du visage.

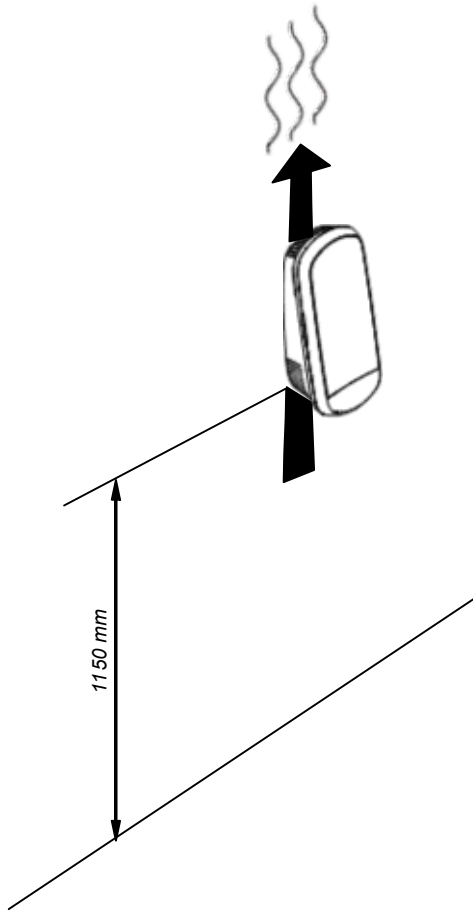
- ◆ Contrôle d'accès et gestion horaire
- ◆ Authentification biométrique du visage
- ◆ Interface homme-machine simple et ergonomique
- ◆ Lecteur sans contact (MIFARE Classic, MIFARE Plus, DESFire, HID® Iclass*, HID® PROX*)
- ◆ Connectivité universelle (Gigabit Ethernet, Wi-Fi™, RS485/422, Wiegand, Dataclock)
- ◆ Capteur de détection d'intrusion

* Selon la version du produit





Installation recommandations / environment



Veuillez installer le terminal VisionPass verticalement à la hauteur recommandée, et laissez les ouvertures libres pour permettre la circulation de l'air.

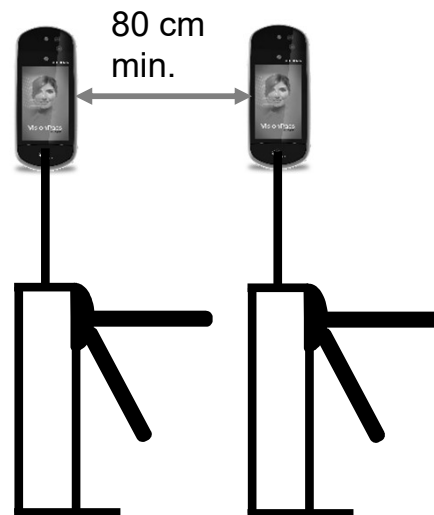
Le terminal VisionPass est conçu pour fonctionner dans la plupart des conditions environnementales. Quoi qu'il en soit, pour optimiser les performances du VisionPass, il est préférable de suivre les règles ci-dessous :

- Évitez que la lumière du soleil ne vienne directement sur l'appareil (par exemple, évitez d'installer l'appareil face à une fenêtre).
- Évitez la lumière directe du soleil sur le visage de l'utilisateur.
- Évitez les forts contrastes gauche/droite ou haut/bas, ainsi que les ombres sur le visage de l'utilisateur dues à la configuration de l'éclairage.
- Préférez un fond de couleur neutre dans le champ de vision du produit
- Évitez tout point lumineux très proche de l'appareil (moins d'un mètre)
- Protégez la vitre avant des gouttes de pluie car elles pourraient affecter les capteurs

NB : Attention, en fonctionnement, le radiateur interne peut être chaud.

Si plusieurs terminaux sont installés sur des voies parallèles (généralement pour les portails ou les tourniquets), une distance minimale de 80 cm doit être respectée entre les terminaux.

Il est également possible d'incliner les terminaux de manière à ce que le champ de vision d'un terminal n'interfère pas avec celui de l'autre.



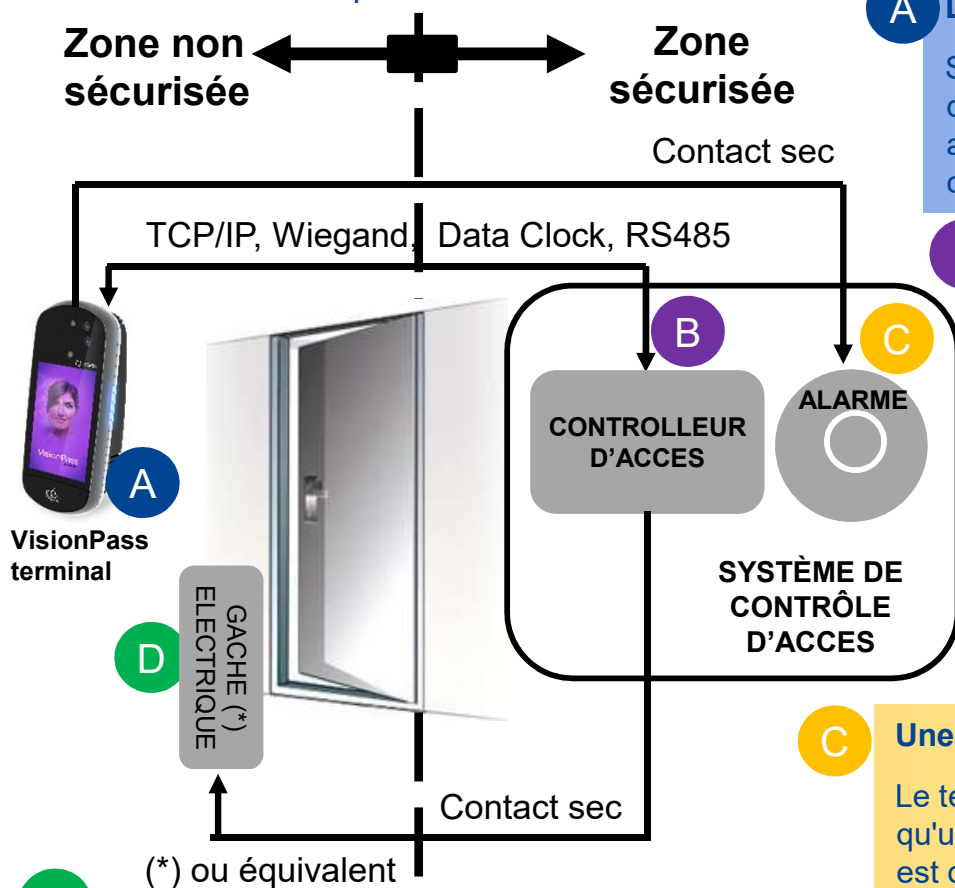
Gardez cette zone propre et dégagée : pas d'autocollant, etc.





Terminal Implementation

To secure an access, IDEMIA recommends installing the VisionPass terminal as a part of a typical Access Control system, which consists of the components described below.



A Le terminal VisionPass

Sa fonction consiste à traiter la demande d'accès de l'utilisateur. Il contrôle les droits d'accès par identification biométrique (avec une base), ou par authentification biométrique, et/ou par authentification d'une carte RFID (et de son contenu), et/ou vérification d'un code PIN..

B Un contrôleur d'accès centralisé (produit tiers)

Le terminal est en interface avec un contrôleur d'accès (via un protocole TCP/IP, Wiegand, Data Clock ou RS485)

Après une demande d'accès, le terminal envoie le résultat des droits d'accès de l'utilisateur au Contrôleur d'accès (ce message contient au moins l'Identifiant de l'utilisateur)

Le Contrôleur d'accès effectue des contrôles supplémentaires et renvoie la décision finale (accès accordé/refusé) au terminal (qui affiche le résultat à l'intention de l'utilisateur) et au contrôleur de porte qui ouvre la porte (si l'accès a été accordé).

C Une alarme (produit tiers)

Le terminal envoie un message au Contrôleur d'accès pour activer l'Alarme dès qu'une action malveillante comme une tentative d'intrusion ou d'arrachement du mur est détectée

D Un verrou électrique de porte ou un dispositif équivalent (produit tiers)

Le Contrôleur d'accès envoie une commande pour activer le verrou si l'accès est accordé (c'est à dire l'identifiant de l'utilisateur est répertorié dans la liste des utilisateur autorisés). Le contrôle du verrou (ou de la gâche) est réalisé par un contact sec.



Processus de contrôle d'accès type



Sur demande d'accès, le terminal vérifie les droits d'accès de l'utilisateur à l'aide d'un contrôle biométrique.

Si le résultat du contrôle est réussi (utilisateur reconnu), un message est envoyé au Contrôleur d'accès central pour d'autres contrôles sur les droits d'accès.

Si l'utilisateur est autorisé à accéder à la zone protégée, le contrôleur d'accès central renvoie un message « accès accordé » au terminal et une commande « d'ouverture » au contrôleur de porte.



Note: Un utilisateur doit être enrôlé dans la base de données du terminal, afin de pouvoir effectuer un contrôle biométrique.



Modes de contrôle d'accès disponibles

Le terminal peut être configuré selon l'un des modes décrits dans le tableau ci-dessous

	Identification	Authentification	Multi facteur	Serveur proxy
Application de contrôle d'accès	Application exécutée sur le terminal au démarrage.	Application exécutée sur le terminal au démarrage.	Application exécutée sur le terminal au démarrage.	Application distante qui pilote le terminal via le réseau
Événement déclencheur de la demande d'accès	L'utilisateur place un doigt sur le capteur biométrique.	L'utilisateur place sa carte sans contact devant le lecteur. (*)	L'utilisateur pose son doigt sur le capteur ou présente sa carte devant le terminal	Les événements déclencheurs sont choisis par l'application à distance
Contrôle biométrique (si activé)	L'empreinte digitale capturée est comparée à toutes les empreintes digitales de la base de données.	L'empreinte digitale capturée est comparée à l'empreinte digitale de référence de l'utilisateur. (**)	Celui de l'identification ou de l'authentification, suivant l'événement déclencheur	Choisi par l'application distance
Décision d'afficher un signal de résultat à l'intention de l'utilisateur	Par application autonome d'identification	Par application autonome d'authentification	Par application autonome exécutée	Par application distante

(*) ou l'utilisateur entre son Identifiant sur le clavier, ou le terminal reçoit une trame Wiegand transmis par un dispositif externe

(**) stockée sur la carte sans contact ou dans l'enregistrement de l'utilisateur dans la base de données locale du terminal



Environnement de déploiement

Température de fonctionnement	-10° to +45 °C (14°to 113°F)
Humidité tolérée en fonctionnement	10 % < RH < 80 % (non condensing)
Température de stockage	-25°to + 70 °C (-13°to 158°F)
Humidité tolérée pour le stockage	5% < RH < 95 %

Précautions générales

- ◆ Ne pas exposer le terminal à des températures extrêmes.
- ◆ Lorsque l'environnement est très sec, éviter toute moquette synthétique à proximité du terminal, afin de réduire le risque de décharge électrostatique indésirable.

Zones contenant des combustibles

- ◆ Ne pas installer le terminal près de postes d'essence ou d'autres installations contenant des gaz ou des matières inflammables ou combustibles. Le terminal n'est pas conçu avec une sécurité intrinsèque.

Le terminal doit être installé dans des conditions d'éclairage contrôlées

- ◆ Eviter toute exposition directe du capteur biométrique à la lumière du soleil.

Le terminal doit être installé dans une zone contrôlée afin d'éviter la présence d'eau sur le capteur.



Aide au placement

VisionPass propose 3 façons de guider l'utilisateur afin de positionner au mieux son visage pour l'identification.



Aucune aide au placement : Le volume d'acquisition du terminal est suffisamment important pour permettre à l'utilisateur d'être facilement reconnu dès qu'il le regarde. Cette méthode est adaptée aux utilisateurs quotidiens.

User Guidance Using Icons : des icônes intuitives indiquent à l'utilisateur de se rapprocher ou de reculer, ou de se déplacer à gauche ou à droite

User Guidance Using Camera : Le terminal affichera un retour live de la caméra



Deliberate trigger

Par défaut, le VisionPass réagit lorsqu'un utilisateur entre dans la zone d'intention, et commence l'acquisition faciale dès qu'un utilisateur entre dans la zone de codage et regarde le terminal. Notez que le flux vidéo n'est jamais enregistré par le VisionPass.

Même si le flux vidéo n'est pas enregistré par le terminal, il peut être demandé de désactiver les caméras lorsqu'elles ne sont pas nécessaires, pour des raisons de protection de la vie privée. Le VisionPass peut être configuré pour activer les caméras uniquement à la demande de l'utilisateur :

Activer le paramètre 'Caméra activée sur demande' dans le Menu Sécurité:



Pour utiliser le terminal, l'utilisateur doit cliquer sur l'icône

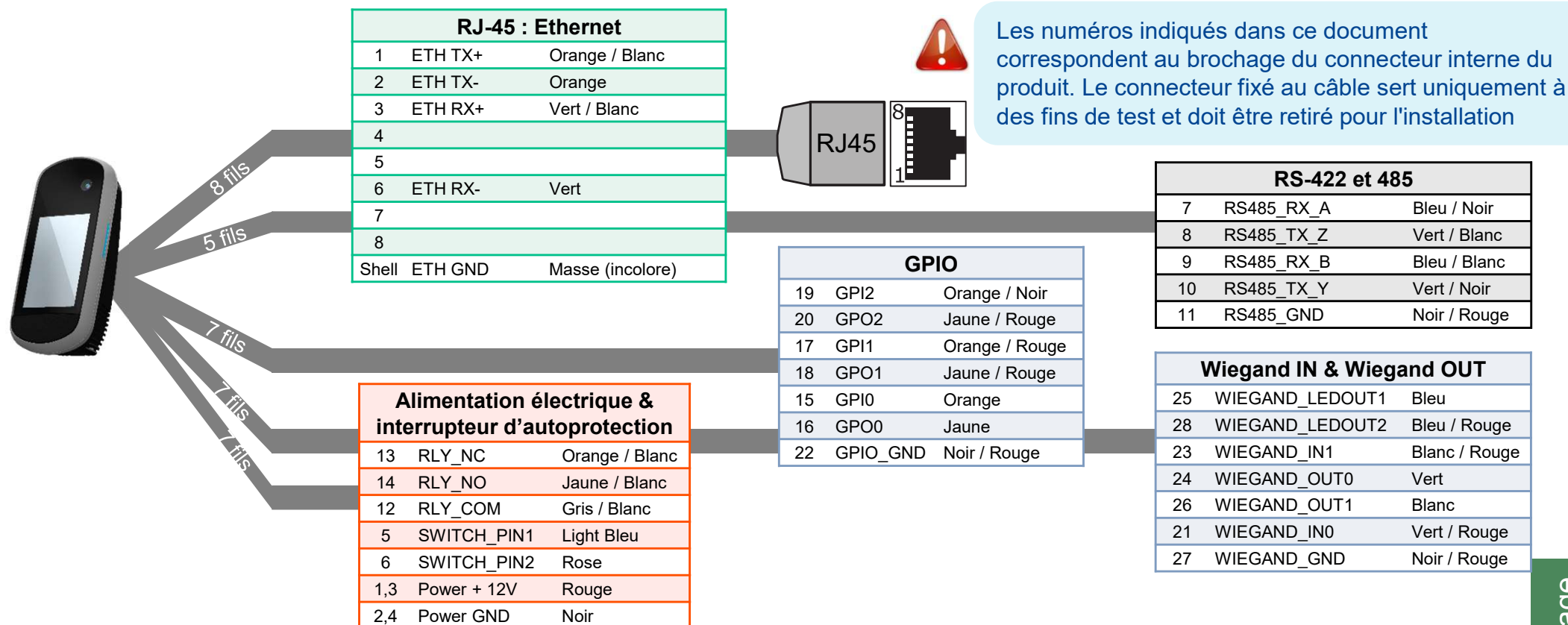


Note : les caméras seront également activées en entrant l'ID sur le clavier ou en présentant une carte sans contact si ces déclencheurs sont activés





Présentation générale du câblage



Toutes les connexions du terminal sont de type TBTS (Très Basse Tension de Sécurité électrique)..

L'alimentation fournie par la source électrique doit être coupée avant de débuter l'installation.

Avant de procéder, s'assurer que la personne en charge de l'installation et des connexions est reliée correctement à la terre afin d'empêcher d'éventuelles décharges électriques (ESD).

Conservation de la Date/Heure du terminal : les réglages volatiles (comme la date/l'heure) du terminal sont protégés contre les pannes électriques au moyen d'un composant dédié pendant au moins 24 heures (à 25 °C) sans alimentation extérieure.



Câblage d'alimentation



1-3	Power + 12V	Rouge
2-4	Power GND	Noir

Alimentation électrique extérieure : 12-24 V (régulée et filtrée) 3A min @12V, conforme à la norme IEC60950-1 ou IEC 62368-1. En cas de partage d'alimentation entre plusieurs terminaux, chaque terminal doit recevoir 3A (par exemple, deux terminaux nécessitent une alimentation de 12 VDC, 6A supply).

Un système de sécurisation de l'alimentation par batterie ou une alimentation sans coupure (UPS, Uninterrupted Power Supply) avec une protection intégrée contre les surtensions sont recommandés.

IDEMIA recommande d'utiliser une alimentation 24V 3A et un câble de jauge AWG16. La tension mesurée sur le connecteur du bornier du terminal doit être égale à 12V-24V (-15% / +10%).

Le terminal a besoin d'une puissance de 36 W quelle que soit la tension d'alimentation.

La chute de tension due à la longueur des câbles doit être prise en compte : le tableau ci-contre donne la longueur maximum entre l'alimentation et 1 seul terminal, selon la jauge de câble et la tension

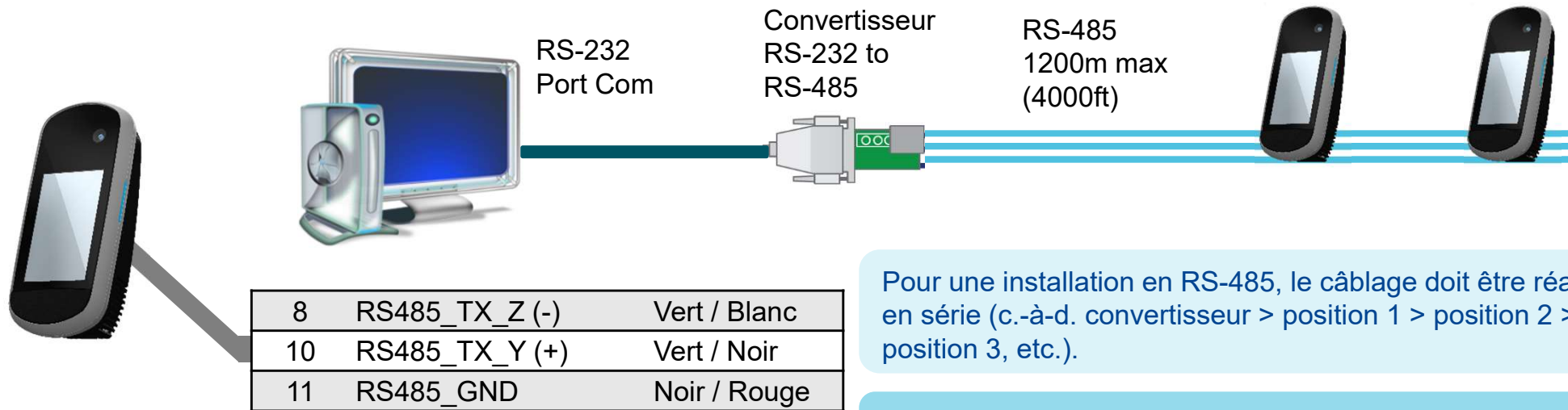
Jauge AWG	Section (mm ²)	Distance maximum selon caractéristiques de l'alimentation			
		12 V +/- 10% 3,6 A	12 V +/- 5% 3,5 A	24 V +/- 10% 2 A	24 V +/- 10% 3 A
16	1.31	6 m	12 m	68 m	121 m
18	0.82	4 m	8 m	43 m	76 m
20	0.52	2 m	5 m	27 m	48 m
22	0.32	1 m	3 m	16 m	30 m



ATTENTION : une alimentation insuffisante peut entraîner une corruption de la mémoire et des données ; de même une surtension peut endommager le matériel. Ces deux anomalies annulent la garantie



Communication RS-485



Pour une installation en RS-485, le câblage doit être réalisé en série (c.-à-d. convertisseur > position 1 > position 2 > position 3, etc.).

Choisir un convertisseur supportant le passage du mode émission à réception (et vice versa) par l'état "idle".

Utiliser un câble CAT-5 UTP (ou de qualité supérieure) (blindé de préférence) avec une impédance caractéristique de 120 ohms. Utiliser un câble de jauge AWG 24 minimum.

Choisir une paire torsadée pour les signaux RS485_TX_Y (TX+, fil Vert / Noir - 10) et RS485_TX_Z (TX-, fil Vert / Blanc - 8). Un autre conducteur doit être utilisé pour la masse du signal (fil Noir / Rouge - 11).

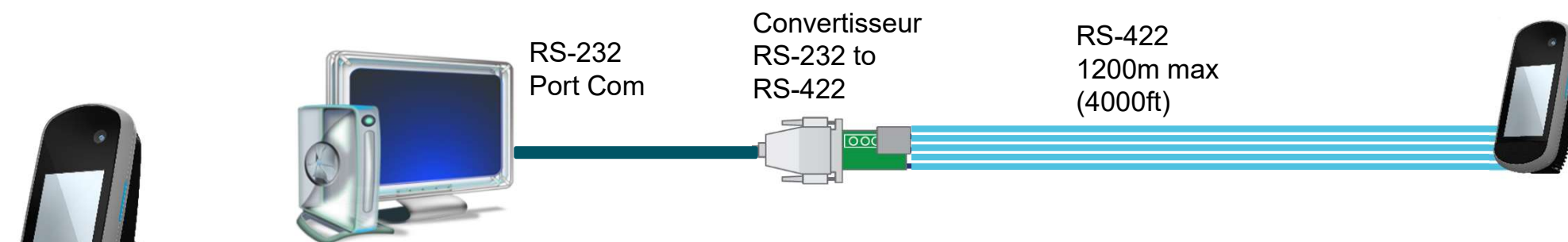
IMPORTANT:

- Jusqu'à 31 dispositifs peuvent être installés au maximum sur une même ligne RS485.
- La longueur de câble totale maximale ne doit pas dépasser 1 200 m (soit 4 000 ft).
- Le câble doit être dédié à cette installation uniquement et non utilisé à d'autres fins.





RS-422 Communication



7	RS485_RX_A (RX+)	Bleu / Noir
8	RS485_TX_Z (TX-)	Vert / Blanc
9	RS485_RX_B (RX-)	Bleu / Blanc
10	RS485_TX_Y (TX+)	Vert / Noir
11	RS485_GND	Noir / Rouge

Pour une installation en RS-422, le câblage doit être réalisé en série (c.-à-d. convertisseur > position 1 > position 2 > position 3, etc.).

Utiliser un câble CAT-5 UTP (ou de qualité supérieure) (blindé de préférence) avec une impédance caractéristique de 120 ohms. Utiliser un câble de jauge AWG 24 minimum.

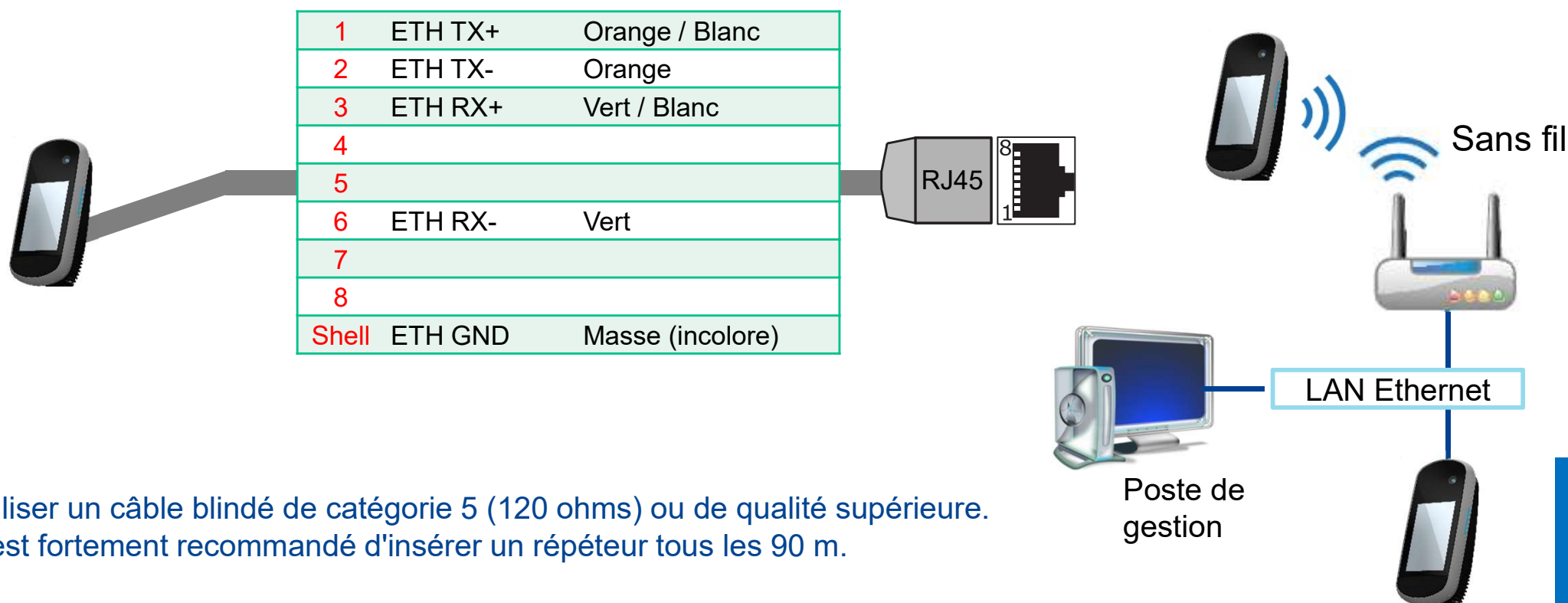
Choisir une paire torsadée pour les signaux RS485_TX_Y (fil TX+, Vert / Noir- 10) et RS485_TX_Z (fil TX-, Vert / Blanc - 8).
Choisir une paire torsadée pour les signaux RS485_RX_A (fil RX+, Bleu / Noir- 7) et RS485_RX_B (fil RX-, Bleu / Blanc- 9).
Un autre conducteur doit être utilisé pour la masse du signal (fil Noir / Rouge - 11).



La longueur de câble totale maximale ne doit pas dépasser 1 200 m (soit 4 000 ft).
Le câble doit être dédié à cette installation uniquement et non utilisé à d'autres fins.



LAN Ethernet et WLAN (sans fil)



Utiliser un câble blindé de catégorie 5 (120 ohms) ou de qualité supérieure.
Il est fortement recommandé d'insérer un répéteur tous les 90 m.

Pardéfaut, le terminal est en mode IP statique (réglage usine) : IP=192.168.1.10,
passerelle=192.168.1.254, masque= 255.255.254.0

Connexion Ethernet sur le bornier

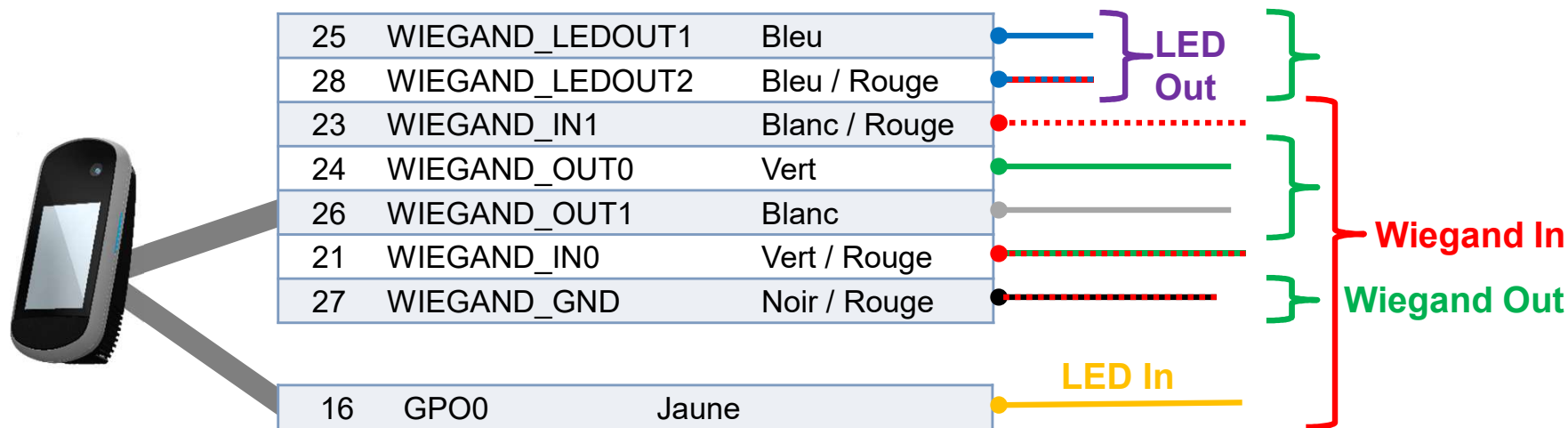
- ◆ Une très grande vigilance est recommandée lors de la connexion du câble Ethernet sur le bornier car une connexion de mauvaise qualité peut dégrader considérablement la sensibilité du signal Ethernet.
- ◆ Brancher Rx+ et Rx- avec les deux fils d'une même paire torsadée (et faire de même pour Tx+/Tx- avec les deux fils d'une autre paire torsadée).

Option WLAN

Les adaptateurs sans fil Idemia prennent en charge les normes 802.11b et 802.11g. WEP Open, WPA et WPA2 sont supportés.



Communication Wiegand



Three-conductor cable (shielded recommended) is required for Data 0, Data 1, and WGND.

Use 18-22 AWG cable in a homerun configuration from each unit to the Access Control Panel (ACP).

- ◆ Brancher **WIEGAND_OUT0** (fil Vert – Pin 24) avec Data 0 de l'ACP
- ◆ Brancher **WIEGAND_OUT1** (fil Blanc – Pin 26) avec Data 1 de l'ACP
- ◆ Brancher **WIEGAND_GND** (fil Noir / Read – Pin 27) avec la borne commune du lecteur de l'ACP (0 VCC).

Pour un câble de jauge 18 AWG, la distance de câble maximale est de 150m (500 ft) ; pour une jauge de 20 AWG, la distance maximale est de 90m (300 ft) ; pour une jauge de 22 AWG, la distance maximale est 60m (200 ft).

Toutes les sorties du contrôleur devront être de type à collecteur ouvert ou 5 V+/-5 %



Communication Wiegand (suite)

Important

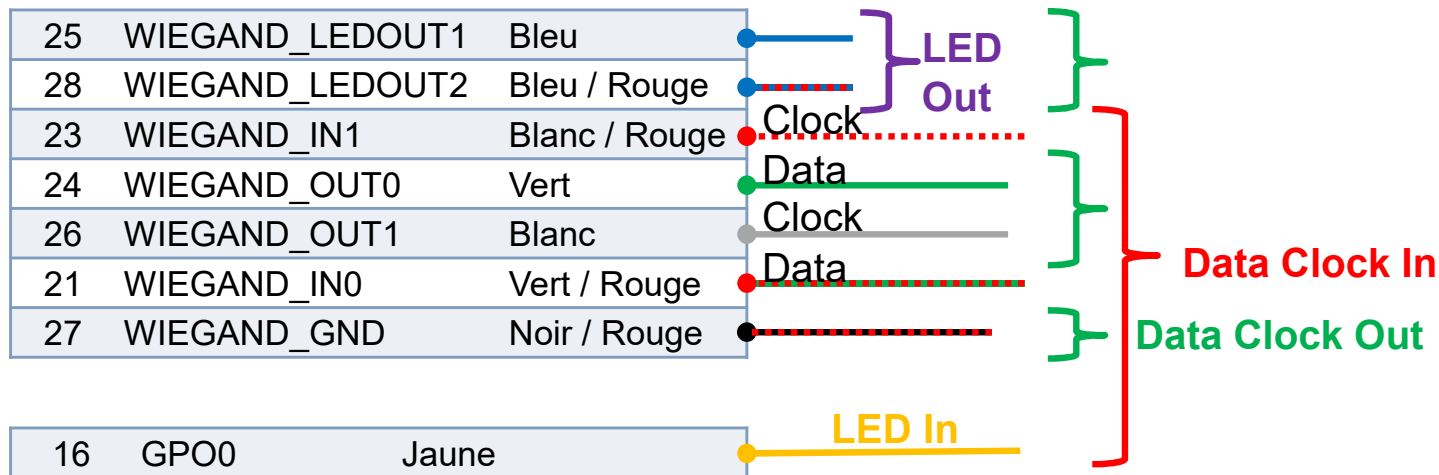
Par défaut, le port de sortie Wiegand n'est pas activé. La sortie Wiegand doit être configurée avant d'effectuer la connexion à l'ACP.

Note

Lors de l'installation, l'administrateur du système sera invité à choisir un format de trame Wiegand préexistant ou à créer un format de trame personnalisé et à le charger dans le terminal avant sa première utilisation.

Data Clock

Le port Wiegand prend également en charge le protocole Clock & Data. Le câblage est décrit ci-dessous.



Exemple d'informations sur le format

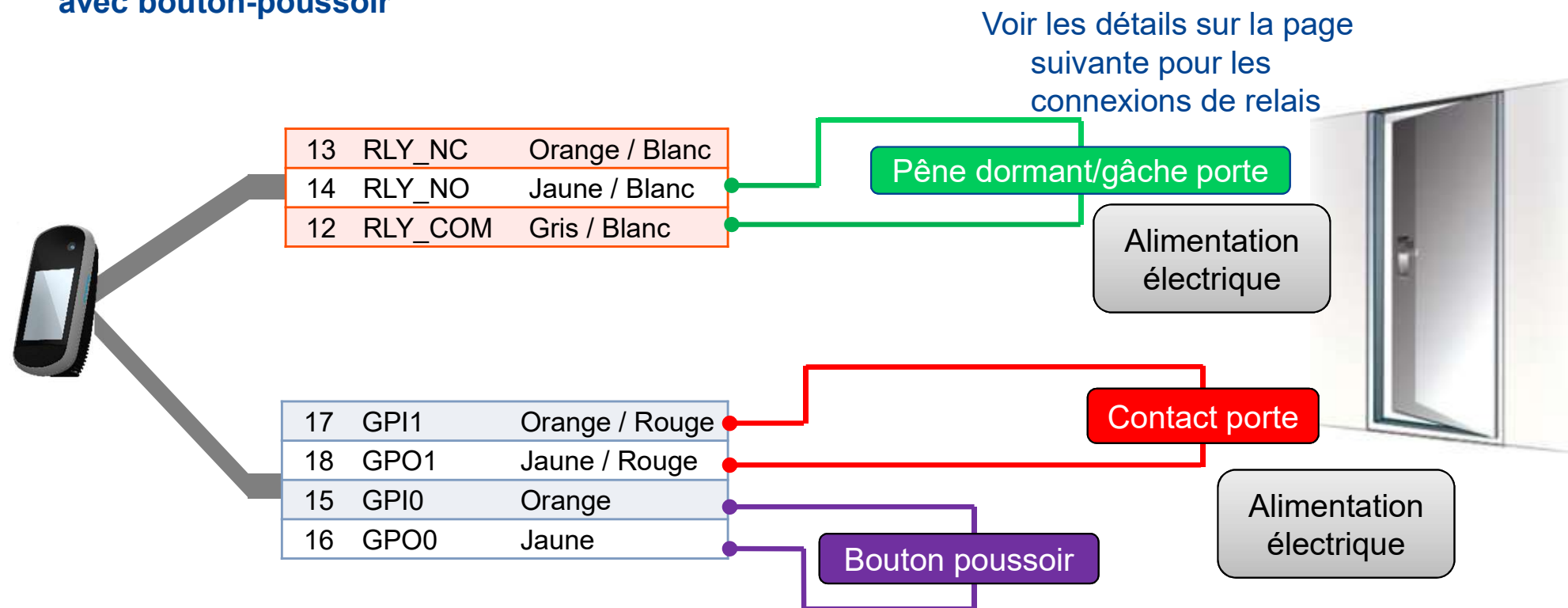
Type : **26 bits standard**

- Plage de code site Alt et de code site Fail : **0 à 255**
- Plage modèle de numéro ID : **1 à 65535**
- Plage étendue de numéro ID : **N/A**
- Bit start ID : 9
- Longueur ID : 16
- Bit start de code site : 1
- Longueur de code site : 8
- Longueur de bit start : 0



Contrôle d'accès de porte unique (SDAC)

Exemple de câblage de Contrôle d'accès de porte unique (SDAC : Single Door Access Control) :
avec bouton-poussoir



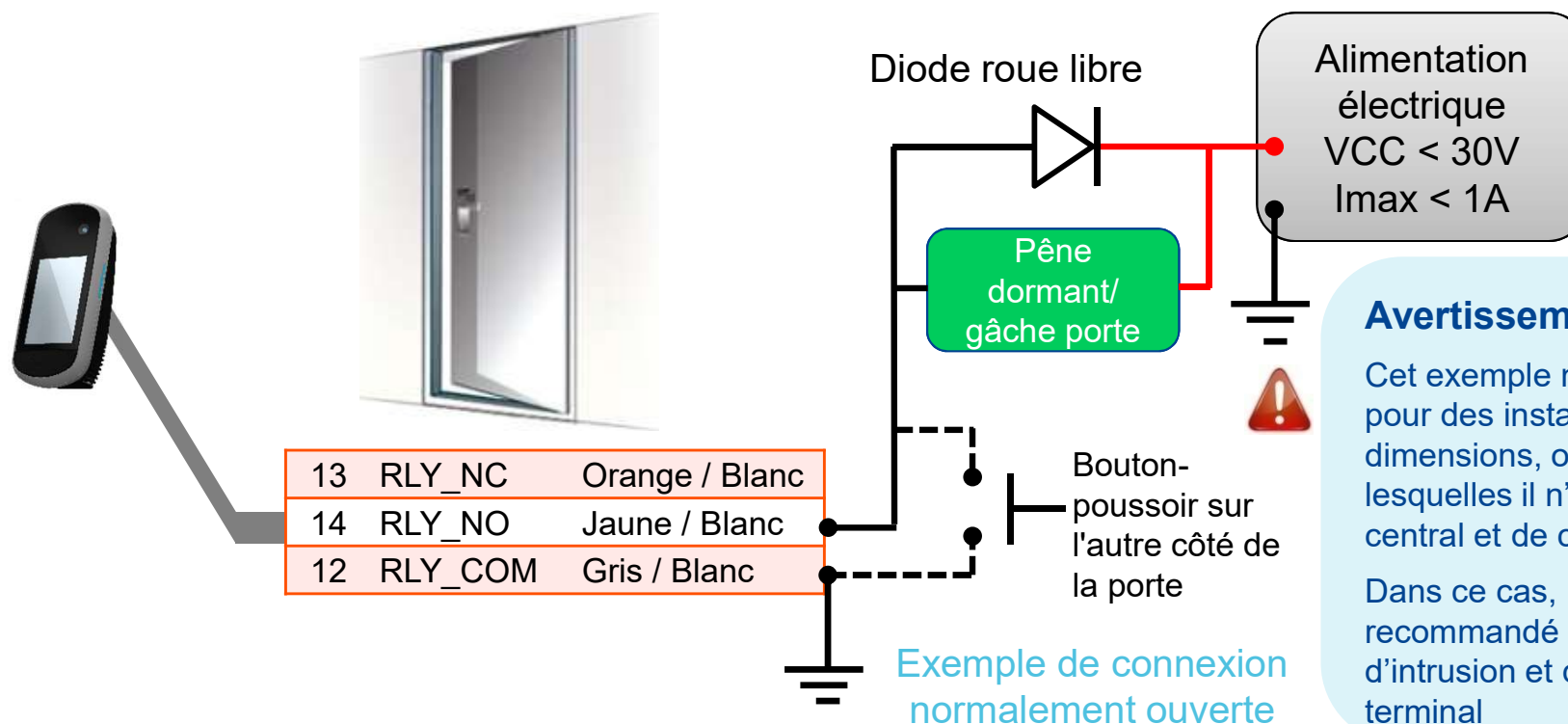
S'il n'y a pas de contact de porte, GPI1 (10) et GPO1 (12) doivent être connectés ensemble



L'alimentation fournie par la source électrique doit être coupée avant de débuter l'installation.



Câblage du relais interne



Avertissement

Cet exemple n'est recommandé que pour des installations de petites dimensions, ou autonomes dans lesquelles il n'y a pas de contrôleur central et de contrôleur de porte.

Dans ce cas, il est fortement recommandé d'utiliser la détection d'intrusion et d'arrachement du terminal

La gestion de la charge inductive nécessite une diode parallèle pour une durée de vie optimale des contacts

Avertissement

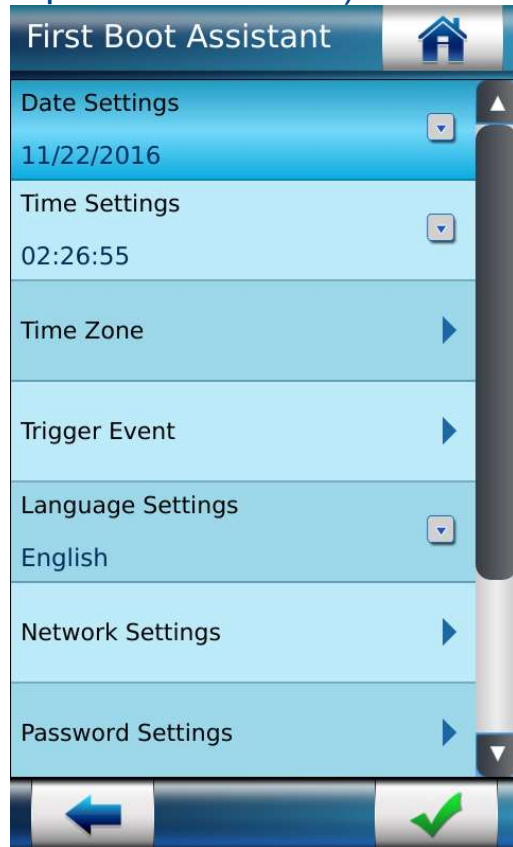
- Le relais interne est limité à un courant maximal de 1 A à 30 V. Si le pêne dormant ou la gâche de la porte ponctionne plus de 1 A, le dispositif peut être endommagé. Si la charge du pêne dormant ou de la gâche de la porte dépasse 1 A, un relais externe doit être utilisé.
- Le relais interne a été conçu pour 100 000 cycles. Si un nombre supérieur de cycles est nécessaire, un relais externe piloté par GPO doit être utilisé.



Administration locale - First Boot Assistant

Le First Boot Assistant (FBA) aide l'administrateur à configurer tous les paramètres fondamentaux de l'appareil.

Il est lancé automatiquement au premier démarrage du terminal, mais peut également être lancé à la demande, via le menu d'administration (c'est-à-dire pour réinitialiser les paramètres principaux du terminal)



Principaux paramètres gérés par le FBA

Date et heure et réglage du fuseau horaire

Événement déclencheur : choix du ou des déclencheur(s) à activer lorsque l'utilisateur demande un accès

Langue : choix de la langue

Configuration réseau : paramètres LAN ou


Configuration mot de passe : modification du mot de passe d'administration du terminal

Assistant au prochain démarrage : affiche cet écran au prochain démarrage



Administration locale – Utilisation du menu de l'écran tactile



Appuyer sur l'icône  pour accéder au menu d'administration (mot de passe par défaut : 12345).



Pour des raisons de sécurité, il est fortement recommandé de changer le mot de passe par défaut de l'appareil.

Icônes utilisées fréquemment



Retour (et Annuler)



Sortir ou retour au menu principal



Annuler



Valider



Administration with MorphoBioToolBox application

Il est également possible de configurer le terminal VisionPass en utilisant une application (pour Windows) dédiée :

MorphoBioToolBox

Veuillez noter que cette application a un Guide de l'utilisateur intégré (Menu Aide).



Administration du terminal via l'application MorphoBioToolBox

Connection

Terminal Type: MA Sigma

Connection information

☒ TCP / IP ☐ Serial

Address type: ☒ IPv4 ☐ IPv6

Address: [text field]

Port: 11010

Timeout: 10 seconds [5-30]

Use SSL / TLS: ☐

Terminal CA certificate path: [text field]

Client certificate path: [text field]

Client certificate password: [text field]

Recent Terminals

Erase logs Export

MBTB Logs

11:34:52 - INFO - Load successful;MBTB.Plugins.RebootFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PingFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PasswordConfigurationTabFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PassphraseConfigurationTabFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.JobCodesTabFeature



Logiciel permettant l'administration à distance du terminal

Les terminaux VisionPass sont compatibles avec l'application MorphoManager (version 14.3 or higher)



MorphoManager





Procédure d'enrôlement local 1/2

Un nouvel utilisateur peut facilement être ajouté en utilisant le menu d'administration du terminal VisionPass. Cet « enrôlement local » n'est recommandé que pour des installations ou des tests de petite taille ou autonomes. Pour les systèmes professionnels, l'enrôlement doit être effectué à distance avec une station d'enrôlement, qui est un PC équipé d'une application dédiée telle que MorphoManager.

Ce menu permet d'ajouter l'enregistrement d'un utilisateur dans la base de données locale, avec la possibilité de créer une carte sans contact d'utilisateur, avec les données de référence de l'utilisateur.

Informations d'enrôlement :

- ◆ Nom et prénom de l'utilisateur
- ◆ Visage de l'utilisateur (données biométriques)
- ◆ Droits administrateur de l'utilisateur (aucun, base de données, complet, droits limités)
- ◆ Code PIN de l'utilisateur
- ◆ Planification des accès
- ◆ Messages dynamiques
- ◆ Délai d'attente de fermeture de porte
- ◆ Date d'expiration
- ◆ Utilisateur sur liste utilisateurs autorisés ou VIP
- ◆ Règles par utilisateur

Note: Voir la section enrôlement de l'utilisateur dans le Guide d'administration du VisionPass.

Informations d'enrôlement

Prénom

Nom

Acquisition du visage

Droits d'administration

Pas de droits administrateur

Code PIN utilisateur

Planification des accès

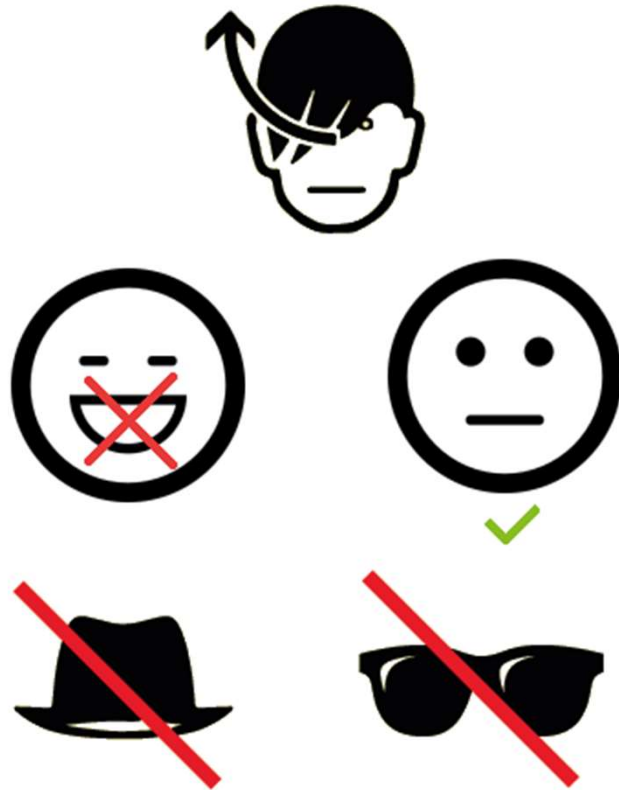
63 : All Access

Soumission aux fermetures site

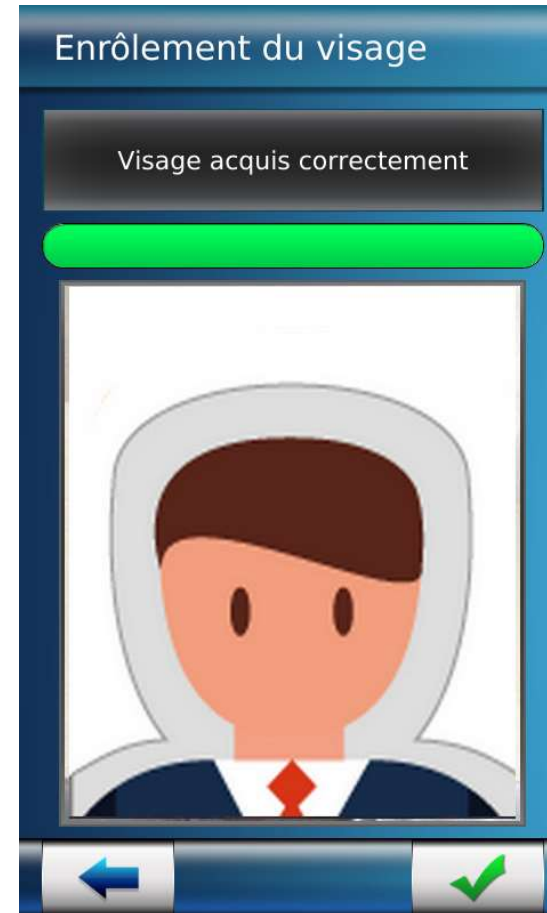
OFF



Procédure d'inscription locale 2/2



Veuillez rester sans bouger devant le produit avec votre visage clairement visible.
Enlevez tous les accessoires.
Enlevez vos lunettes.





Position de la carte sans contact – Entrée du code PIN

Position de la carte sans contact



Cette action est requise une fois au cours du processus d'enrôlement de l'utilisateur (génération / encodage d'une carte), et à chaque authentification.

Placez la carte de l'utilisateur devant le lecteur de carte sans contact qui se trouve au niveau du logo 'sans contact'.

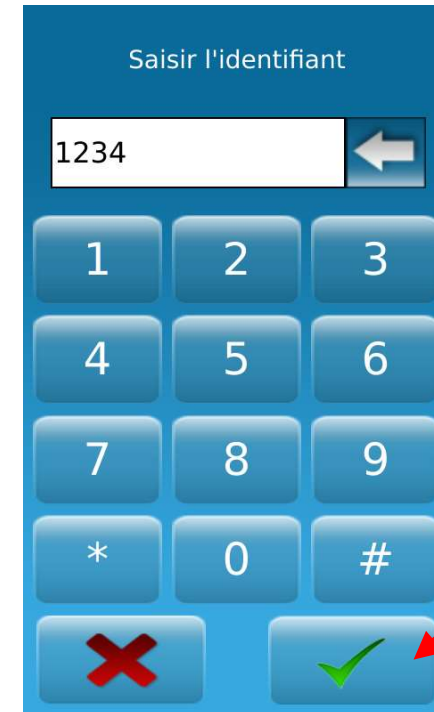


L'authentification de l'utilisateur est déclenchée suite à la détection d'une carte utilisateur par le lecteur de carte sans contact.

Le terminal lit les données de l'utilisateur mémorisées dans la carte (au moins l'ID de l'utilisateur) et débute le processus d'authentification suivant les réglages du terminal.

NB : Le temps nécessaire pour lire toutes les données de la carte sera plus ou moins long selon la quantité de données à extraire et le type de carte.

Entrer le code PIN



Lorsque les réglages du terminal l'y invitent, l'utilisateur doit saisir son code PIN: une fois au cours du processus d'enrôlement, puis lors de chaque authentification (en plus ou à la place du contrôle biométrique).

L'utilisateur saisi son code PIN à l'aide d'un clavier numérique affiché sur l'écran tactile LCD



Fonction de gestion des temps

Le terminal VisionPass intègre une fonction de gestion des temps, optionnelle.

A cet effet, le terminal ajoute des informations spécifiques à chaque enregistrement d'identification ou d'authentification dans la base de données intégrée du journal des événements.

Ces informations sont fournies par l'utilisateur par le biais d'un écran spécifique affiché lors du processus d'identification ou d'authentification.

Cet écran affiche 4 touches de fonction dédiées :

- ◆ Entrée
- ◆ Sortie
- ◆ Début d'une tâche
- ◆ Fin d'une tâche

L'utilisateur doit appuyer sur l'une des touches pour fournir les informations de gestion horaire au terminal.

Cet écran s'affiche après le contrôle biométrique de l'utilisateur ou la lecture de la carte sans contact devant le lecteur.

Un mode étendu est également disponible avec 16 touches de fonction.





Recommandations

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

Réparation and Accessoires

- ◆ Ne pas essayer de réparer le terminal VisionPass par vous-même. Le fabricant ne peut pas être tenu responsable en cas de dommage/d'accident résultant de tentatives de réparation des composants. Toute intervention réalisée par un personnel non autorisé annulera la garantie.
- ◆ N'utiliser le terminal qu'avec ses accessoires d'origine. Des tentatives d'utilisation d'accessoires non approuvés avec le terminal annulera la garantie.

Terminaux non connectés au réseau

- ◆ Pour les terminaux utilisés en mode autonome, il est fortement recommandé de sauvegarder régulièrement la base de données locale, et au moins après des changements importants dans la base de données (ajout, suppression ou modification des utilisateurs), sur un support externe tel qu'une clé de stockage de masse.

Synchronisation de la date et de l'heure

- ◆ L'horloge interne du terminal VisionPass a une précision de +/- 10 ppm à +25°C (soit environ +/- 1sec par jour). A des températures inférieures ou supérieures, l'écart peut être supérieur (maximum : 8 secondes pour 48 heures).
- ◆ Si le terminal est utilisé pour des applications nécessitant une grande précision horaire, nous vous recommandons de synchroniser régulièrement l'heure du terminal avec une horloge externe.

Précautions pour le nettoyage

- ◆ Un tissu sec doit être utilisé pour nettoyer le terminal, notamment la vitre devant le capteur biométrique.
- ◆ L'utilisation de liquides acides, d'alcool ou de matériaux abrasifs est interdite.
- ◆ Utilisez un spray d'air sec pour enlever la poussière du verre du capteur

Version de logiciel

- ◆ Pour tirer le meilleur parti de notre technologie, nous vous recommandons de télécharger et d'installer la dernière version du logiciel (veuillez vous référer à la dernière page)



Documentation

Documents sur l'installation du terminal

VisionPass Installation Guide, Ref. 2019_2000045728

Ce document décrit la procédure de montage physique des terminaux, les interfaces électriques et les procédures de connexion.

Documents sur l'utilisation et l'administration du terminal

VisionPass - Guide d'Utilisation Rapide, Ref. 2020_2000049237 (ce document)

Ce document donne un aperçu rapide du produit et des bases de la configuration et de l'utilisation.

Biometric terminals Administration Guide, Ref. 2018_2000036794

Ce document décrit les différentes fonctions disponibles sur le terminal et les procédures de configuration du terminal. Il contient également la description complète de tous les paramètres de configuration du terminal.

MWC - VisionPass Parameters Guide, Ref. 2018_2000035285

Ce document contient la description complète de tous les paramètres de configuration du terminal.

Documents pour les développeurs

MorphoAccess 5G Series Host System Interface Specification, Ref. 2016_2000022602

Ce document décrit les commandes supportées par le terminaux biométriques Idemia.

MorphoAccess 5G Series Remote Message Specification, Ref. 2016_2000022373

Ce document décrit le format des messages envoyés par le terminal à un système distant.

Note de version: pour chaque version de logiciel, une note de version est publiée décrivant les nouvelles fonctionnalités, les produits supportés, les problèmes potentiels connus, les limitations de mise à niveau, les recommandations, les restrictions potentielles...



Contacts

Support technique et Hotline

Amérique du Nord

Mail: support.bioterminals.us@idemia.com

Tel: +1 888 940 7477

Amérique du Sud

Mail: support.bioterminals.us@idemia.com

Tel: +1 714 575 2973

Europe, Moyen-Orient, Afrique

Mail: support.bioterminals@idemia.com

Tel: +33 1 30 20 30 40

Asie, Pacifique

Mail: support.bioterminals.in@idemia.com

Tel: +91 1800 120 203 020

Pour connaître les dernières nouveautés en matière de logiciels, de documents et d'informations, veuillez consulter notre site web :

www.biometric-terminals.com

Pour obtenir votre identifiant et votre mot de passe, veuillez contacter votre représentant commercial.

Copyright © 2020, IDEMIA. Tous droits réservés.

www.idemia.com

Toute reproduction totale ou partielle, sous quelque forme ou support que ce soit, est interdite sans l'autorisation écrite expresse d'IDEMIA. Les marques identifiées ici sont des marques déposées par IDEMIA ou par d'autres tiers.