A0U586C

Serrure KelNet@

NOTICE D'UTILISATION

FICHET

Copyright

Serrure KeINet@ – Notice d'utilisation
A0U586C – 100038766 – Ed. 04 - NEX – Septembre 2020

PROTECTION DE L'ENVIRONNEMENT

Conformément à la directive 2012/19/UE relative aux Déchets d'Equipements Electriques et Electroniques (DEEE), ce produit une fois en fin de vie ne doit pas être mêlé aux ordures ménagères mais doit faire l'objet d'une collecte sélective permettant le recyclage.

Cette action contribue à la protection de l'environnement.

L'emballage carton de ce produit est recyclable.

RoHS

Produit conforme à la Directive 2011/65/UE (RoHS).

GARANTIE

Ce produit est garanti un an sous condition de l'avoir installé suivant la présente notice.

En cas de retour du produit, il doit être conditionné dans un emballage similaire à celui d'origine.

Dans le cas d'une carte électronique, celle-ci doit être glissée dans un sachet antistatique la prémunissant contre les décharges électrostatiques.

LECTURE DU DOCUMENT

Attention : Ce symbole indique un point sur lequel porter une attention particulière.

Information : Conseils importants d'utilisation et informations.

Fichet Technologies
Fichet Group
23 route de Schwobsheim
B.P. 40285 Baldenheim
67606 Sélestat Cedex – France

Visiting address:
7 rue Paul Dautier
78140 Vélizy-Villacoublay – France

www.fichetgroup.com

Sommaire

1 PRESENTATION

KelNet@ est une serrure électronique Haute Sécurité certifiée « Système Distribué » qui permet de sécuriser l'accès aux valeurs continues dans les coffres et les chambres fortes

Composants KelNet@ :

- **Unité de saisie (IU) :**

  Terminal qui permet la saisie des codes et le paramétrage des serrures.

  Un terminal permet de piloter de 1 à 16 Unités de Sécurité.

- **Unité de Sécurité (SU) :**

  Il existe deux types de SU :

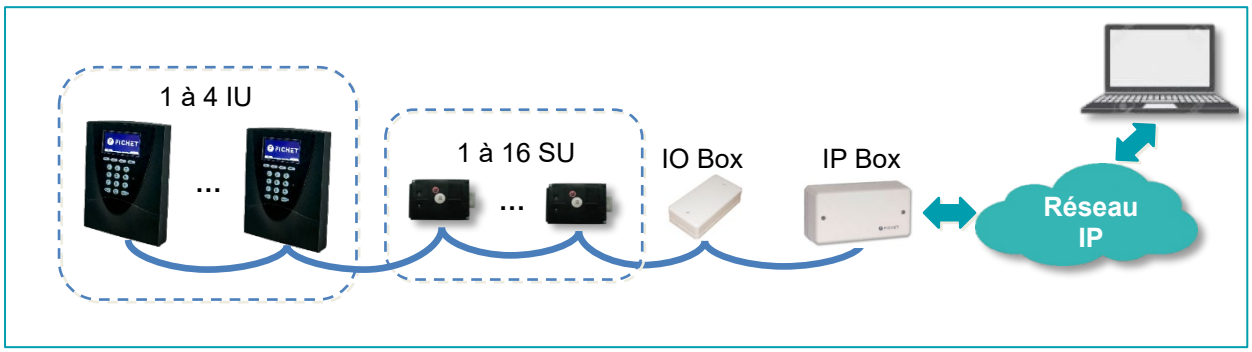
  - **SU standard (SU) :**

    Composant permettant de bloquer le mécanisme de verrouillage de la porte du coffre.

  - **SU Redondante (SU-R) :**

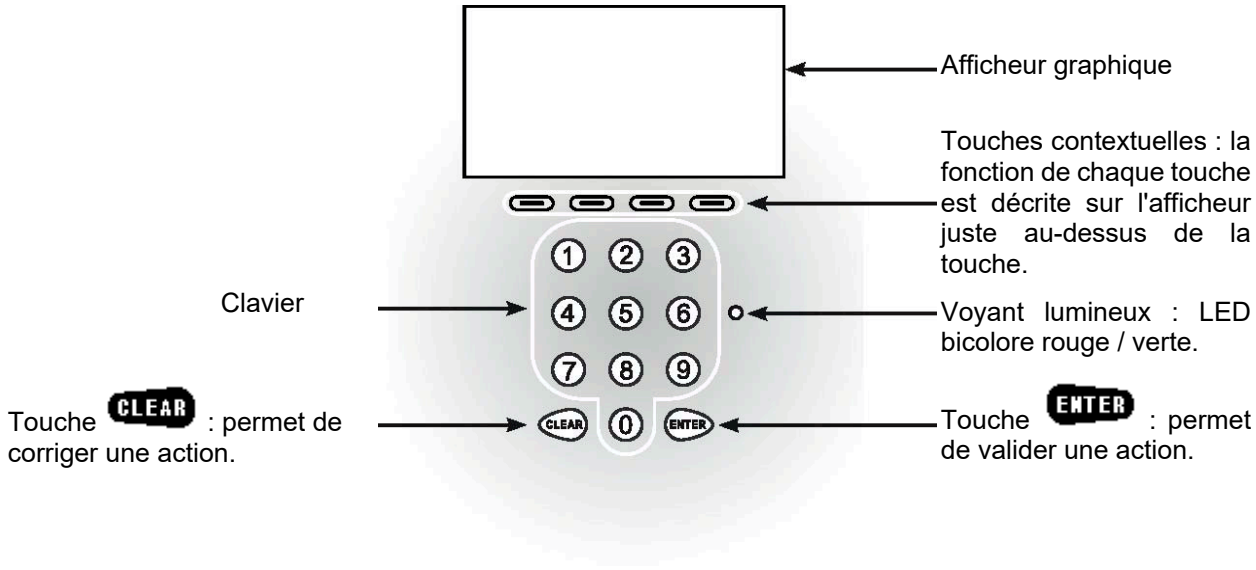
    La SU-R renforce au maximum la fiabilité du système par duplication de l'électronique de la carte, du moteur et des bus de communication.

Le **système distribué** dans son ensemble peut être présenté de la manière suivante :



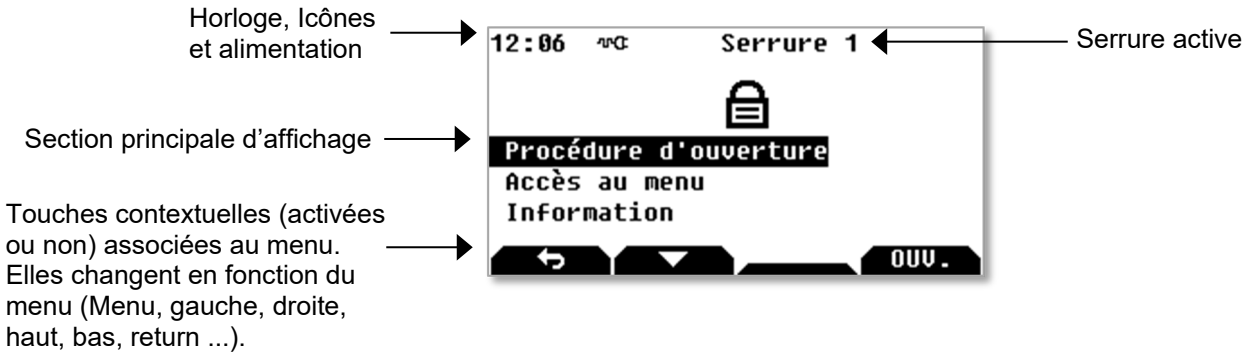
2 DESCRIPTION DU PRODUIT

2.1 Terminal



2.2 Afficheur graphique

2.2.1 Zones graphiques



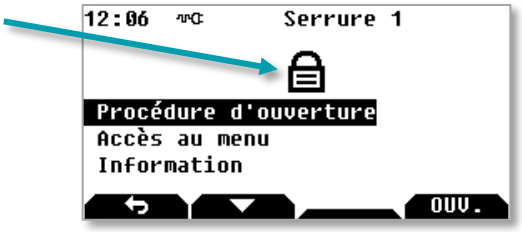
2.2.2 Icônes de statut

Alimentation sur piles ou piles faibles

Alimentation externe

Mauvaise identification (une clé par tentative)

2.2.3 Icônes de menu



Unité de sécurité verrouillée

Unité de sécurité déverrouillée

Empreinte digitale

Identification simple

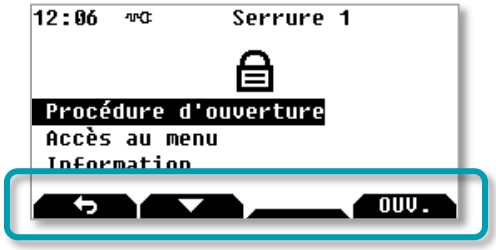
Identification 4 yeux

Alerte – Cette icône est utilisée pour l'affichage des messages système.

Appuyez sur ENTER pour continuer la procédure en cours.

Indique que les convoyeurs (ou tout utilisateur avec procédure anti-passback CIT) sont passés. L'icône reste affichée jusqu'à l'utilisation d'un autre code.

2.2.4 Touches contextuelles



- Gauche
- Droite
- Haut
- Bas
- Retour à l'écran précédent
- Entrée ou validation d'une modification
- OUV. Lancer la procédure d'ouverture (traduit pour chaque langue)
- FERM. Lancer la procédure de fermeture (traduit pour chaque langue)
- -1 Décrémentation de 1
- +1 Incrémentation de 1
- ON Activation
- OFF Désactivation
- OUI Pour valider une action (traduit pour chaque langue)
- NON Pour annuler une action (traduit pour chaque langue)
- Sans fonction

2.3 Sons

La serrure est équipée d'un buzzer :

- d'intensité ajustable
- de durée et de fréquence définissables dans la liste des messages

2.4 Alimentation

2.4.1 Piles et/ou alimentation externe

La serrure peut être alimentée avec :

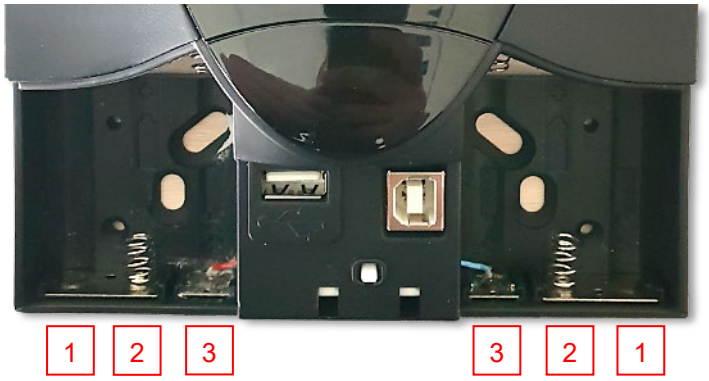
- des piles uniquement,
- des piles et une alimentation externe,
- une alimentation externe uniquement.

Les piles de l'Unité de saisie permettent d'alimenter l'Unité de saisie avec, au plus, 2 Unités de Sécurité locales.

Si la serrure est alimentée avec des piles et une alimentation externe :

- Vérifiez périodiquement les piles. Les remplacer dès qu'un message de piles faibles apparaît.
- Quand l'alimentation externe est coupée, la serrure bascule automatiquement sur l'alimentation par piles.

2.4.2 Installation des piles



- Type de piles : 6 x AAA (LR6) 1,5V.
- Respectez la polarité.
- Installez les piles dans l'ordre suivant : 1 , 2 , puis 3 .

3 UTILISATION DE LA SERRURE

3.1 Catégories d'utilisateurs

Les utilisateurs sont répartis en 3 catégories :

- **Super Managers** : il ne peut y avoir que 2 Super Managers. Les Super Managers ont les droits sur les Managers.

  Chaque Super Manager peut changer le code d'un autre Super Manager sur l'Unité de saisie.
- **Managers** : les Managers peuvent avoir des droits sur les opérateurs.
- **Opérateurs** : les utilisateurs « standards » de la serrure.

3.2 Paramètre d'identification

Un utilisateur est identifié par :

- Son numéro d'identifiant ou « ID ».
- Son code PIN de 6 à 10 chiffres :
  - Pour la classe B, la longueur minimum est de 6 chiffres.
  - Pour la classe C, la longueur minimum est de 7 chiffres.
  - Pour la classe D, la longueur minimum est de 8 chiffres

Super Managers :
- Identifiant (ID) : 1 ou 2
- Code par défaut : 00000000.

Différents modes d'identification sont possibles :

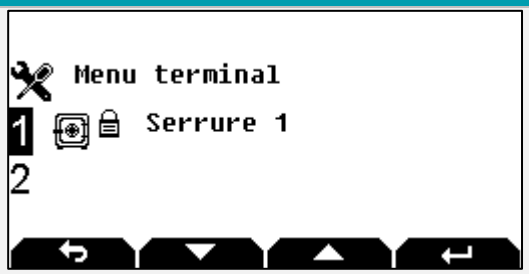
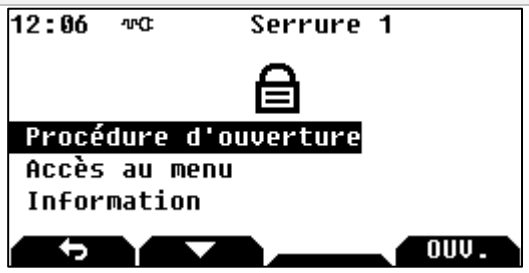
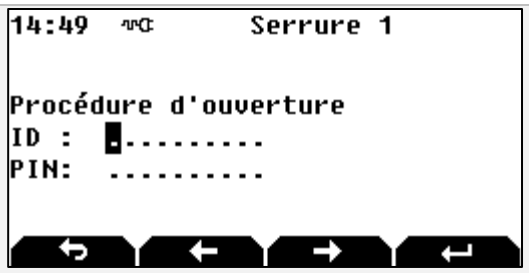
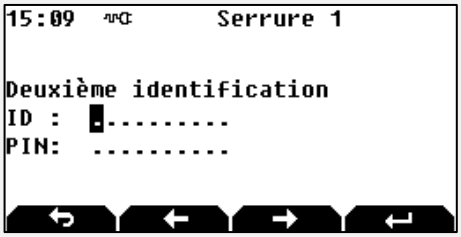
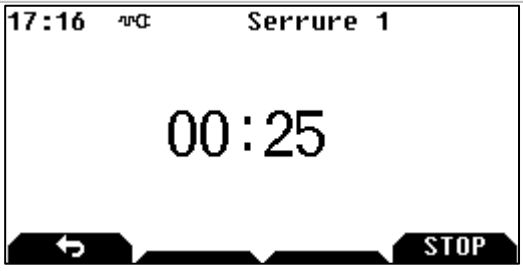
- **Code seul** :
  - Entrez votre numéro d'identifiant et validez par la touche ENTER
  - Entrez votre code PIN et validez par la touche ENTER

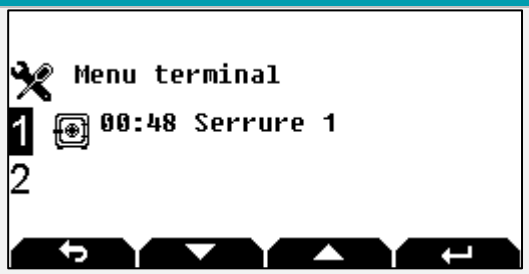
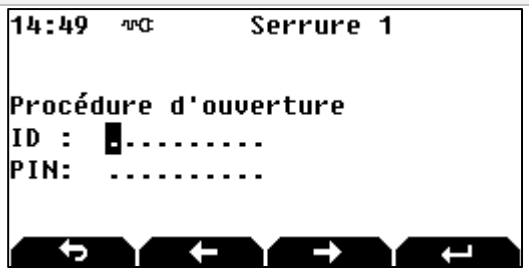
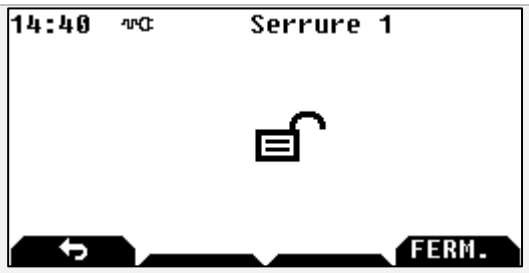
- **Code + Empreinte (optionnel)** :
  - Entrez votre numéro d'identifiant et validez par la touche ENTER
  - Entrez votre code PIN et validez par la touche ENTER
  - Quand le code est validé, la lecture de l'empreinte digitale est demandée : glissez votre doigt sur le capteur biométrique

Voir Chapitre 7 « EMPREINTE DIGITALE » pour plus de détails.

Il est possible de configurer une serrure avec identification par empreinte seule (sans code). Ceci n'est autorisé qu'avec une serrure sans certification, disponible sur demande uniquement.

3.3 Procédure d'ouverture (serrure classe B)

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Appuyez sur ENTER ou sur le bouton OUV. pour lancer la procédure d'ouverture.
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER Un code correct est constitué d'au moins 6 chiffres (max 10 chiffres). Si une empreinte digitale est liée à l'utilisateur, elle sera demandée (voir procédure "Empreinte digitale"). Suivant la configuration de la serrure, il est possible que l'ouverture nécessite une procédure « 4 yeux » (identification de deux utilisateurs différents). Dans ce cas, un deuxième code est demandé :  Si une empreinte digitale est liée à l'utilisateur, elle sera demandée (voir procédure "Empreinte digitale").
4		Attendez si un retard a été défini dans le menu retards et utilisé dans un planning, sinon passez à l'étape **9**.

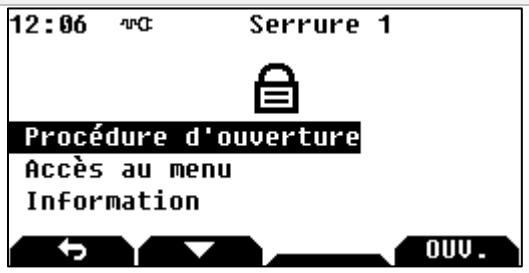
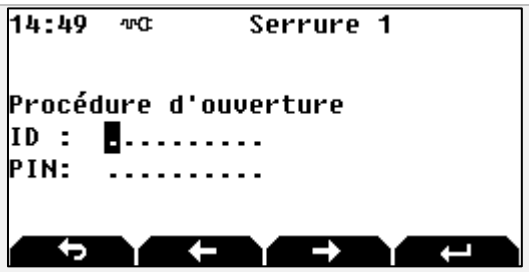
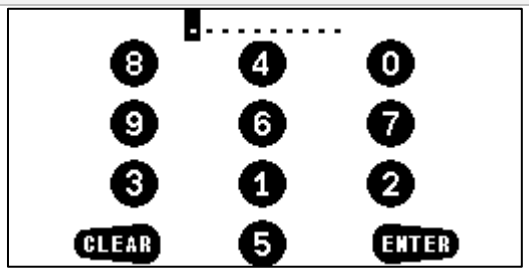
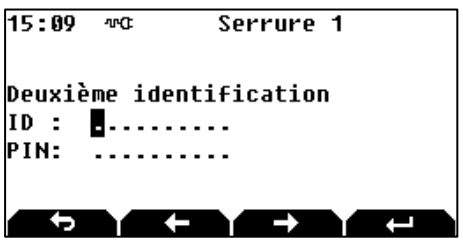
Etape	Ecran	Description
5		Si l'on revient à l'écran d'accueil, on visualisera l'état de toutes les serrures.
6		L'écran d'accueil ci-contre indique qu'une ré-identification est nécessaire. Sélectionnez la serrure + ENTER
7		Sélectionnez **Procédure d'ouverture** + ENTER ou le bouton OUV. pour continuer la procédure d'ouverture, ou **Procédure de fermeture** pour l'abandonner.
8		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER C'est le deuxième utilisateur qui doit entrer son identifiant et son code.
9		La serrure est déverrouillée.
10		L'écran d'accueil ci-contre indique que la serrure est déverrouillée.

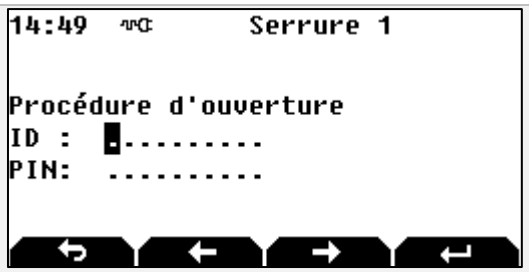
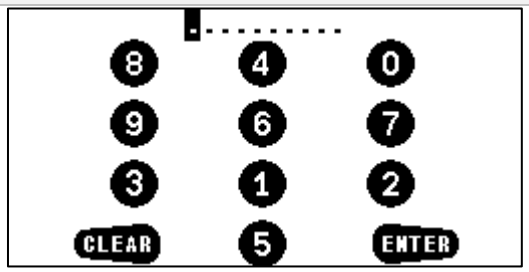
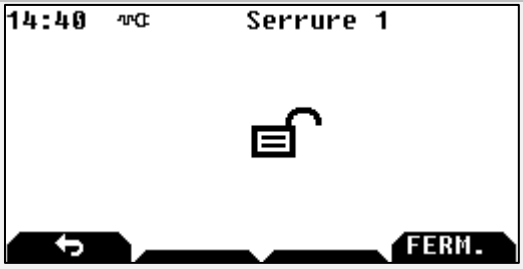
Quand la procédure d'ouverture est lancée, si aucune saisie n'est faite sur le clavier avant 20 secondes, la procédure d'ouverture est abandonnée, et l'on revient à l'écran d'accueil.

Le code d'ouverture est confidentiel et doit être saisi exclusivement dans un environnement sécurisé.

3.4 Procédure d'ouverture (serrure classe C ou D)

Dans le cas d'une **serrure classe C ou D**, la saisie du code ne peut se faire qu'en **mode aléatoire**.

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Appuyez sur ENTER ou sur le bouton OUV. pour lancer la procédure d'ouverture.
3		Tapez votre identifiant + ENTER
4		Tapez votre code via le clavier virtuel + ENTER Dans cet exemple, la touche 1 du clavier correspond au chiffre 8, la touche 2 au chiffre 4, etc. La position des chiffres sur le clavier virtuel change à chaque affichage. Un code correct est constitué d'au moins 7 chiffres pour la classe C et 8 pour la classe D (max 10 chiffres). Si une empreinte digitale est liée à l'utilisateur, elle sera demandée (voir procédure "Empreinte digitale"). Suivant la configuration de la serrure, il est possible que l'ouverture nécessite une procédure « 4 yeux » (identification de deux utilisateurs différents). Dans ce cas, un deuxième code est demandé :  Si une empreinte digitale est liée à l'utilisateur, elle sera demandée (voir procédure "Empreinte digitale").

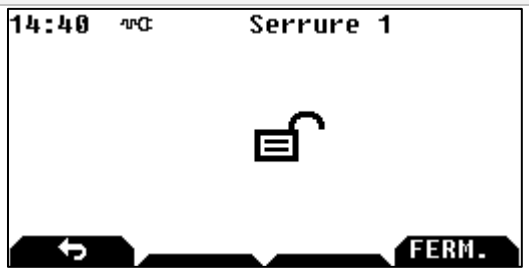
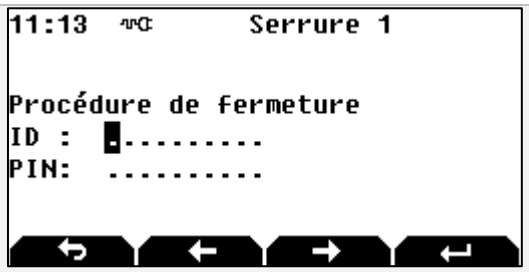
Etape	Ecran	Description
5		Attendez si un retard a été défini dans le menu retards et utilisé dans un planning, sinon passez à l'étape **10**.
6		Si l'on revient à l'écran d'accueil, on visualisera l'état de toutes les serrures.
7		L'écran d'accueil ci-contre indique qu'une ré-identification est nécessaire. Sélectionnez la serrure + ENTER
8		Sélectionnez **Procédure d'ouverture** + ENTER ou le bouton OUV. pour continuer la procédure d'ouverture, ou **Procédure de fermeture** pour l'abandonner.
9		Tapez votre identifiant + ENTER Tapez votre code PIN+ ENTER C'est le deuxième utilisateur qui doit entrer son identifiant et son code.
10		Tapez votre code via le clavier virtuel + ENTER Dans cet exemple la touche 1 du clavier correspond au chiffre 8, la touche 2 au chiffre 4, etc. La position des chiffres sur le clavier virtuel change à chaque affichage.
11		La serrure est déverrouillée.

Quand la procédure d'ouverture est lancée, si aucune saisie n'est faite sur le clavier avant 20 secondes, la procédure d'ouverture est abandonnée, et l'on revient à l'écran d'accueil.

Le code d'ouverture est confidentiel et doit être saisi exclusivement dans un environnement sécurisé.

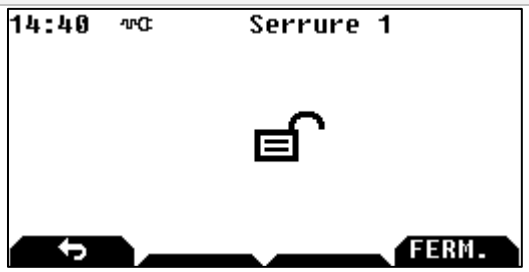
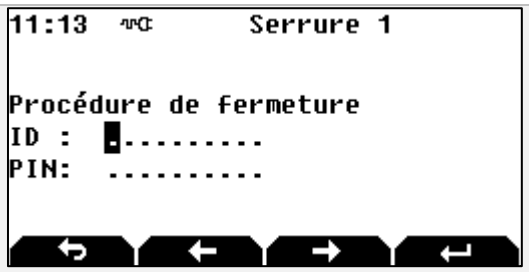
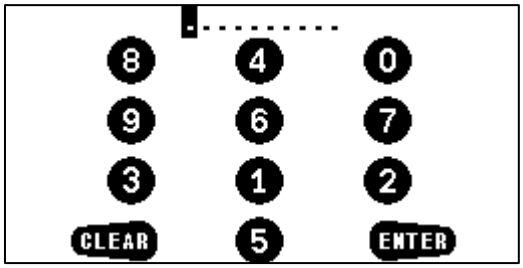
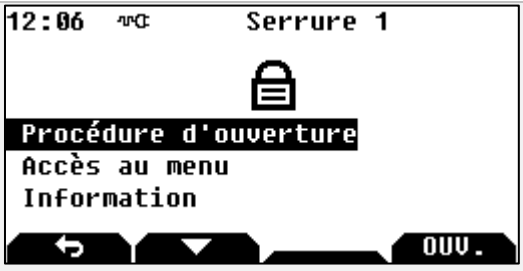
3.5 Procédure de fermeture (serrure classe B)

- **Automatique** : si le switch de tringlerie est connecté, la serrure se verrouille automatiquement lorsque la tringlerie est revenue dans sa position de blocage.
- **Manuelle** : en suivant la procédure ci-dessous.

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Appuyez sur ENTER ou sur le bouton FERM. pour lancer la procédure de fermeture.
3		Si la fermeture par identification a été activée : Tapez votre identifiant + ENTER et votre code PIN + ENTER, sinon passez à l'étape **4**. Dans le cas où un utilisateur doit s'identifier avec son empreinte, celle-ci ne lui sera pas demandée pour la fermeture.
4		La serrure est verrouillée.

3.6 Procédure de fermeture (serrure classe C ou D)

- **Automatique** : si le switch de tringlerie est connecté, la serrure se verrouille automatiquement lorsque la tringlerie est revenue dans sa position de blocage.
- **Manuelle** : en suivant la procédure ci-dessous.

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Appuyez sur le bouton FERM. pour lancer la procédure de fermeture.
3		Si la fermeture par identification a été activée : Tapez votre identifiant + ENTER, sinon passez à l'étape **5**.
4		Tapez votre code via le clavier virtuel + ENTER Dans cet exemple, la touche 1 du clavier correspond au chiffre 8, la touche 2 au chiffre 4, etc. La position des chiffres sur le clavier virtuel change à chaque affichage. Dans le cas où un utilisateur doit s'identifier avec son empreinte, celle-ci ne lui sera pas demandée pour la fermeture.
5		La serrure est verrouillée.

3.7 Blocage d'urgence

En cas d'urgence, appuyez simultanément les touches 7 + 9 pour sécuriser la porte et pour bloquer les ouvertures pendant 30 mn (paramétrable de 1 à 99 mn).

Il n'est pas possible de changer la combinaison des touches du blocage d'urgence.

3.8 Procédure d'anti-passback CIT

Cette procédure permet de limiter l'utilisation d'un code en temps et en nombre d'ouvertures consécutives.

Si l'anti-passback est activé dans le mode « CIT » :

- La première saisie du code permet l'ouverture et lance une temporisation définie au préalable dans l'Outil de Configuration.
- Ensuite, le même code peut être utilisé plusieurs fois dans une limite définie au préalable dans l'Outil de Configuration.
- Une fois le nombre maximum de saisies du code atteint ou à l'échéance de la temporisation, le code n'est plus utilisable.

Le code est réactivé par une identification d'un utilisateur d'un autre groupe de droits.

Dès lors que la temporisation d'anti-passback CIT est lancée, toutes les autres demandes d'ouverture et les accès au menu sont interdits jusqu'à son échéance.

Si un code est saisi dans cette période, le message « **Anti-passback actif** » apparaît.

Une fois le nombre maximum de saisies du code atteint ou à l'échéance de la temporisation, l'icône apparaît pour indiquer que le code anti-passback n'est plus utilisable et que tous les autres codes sont à nouveau utilisables.

L'icône disparaît après identification d'un utilisateur d'un autre groupe de droits.

Tant que le code en anti-passback CIT n'est pas réarmé (par un code utilisateur), le message « **Code non validé** » s'affiche si le code est saisi.

3.9 Règles de blocage faux code

Il y a 2 règles définissant le temps de blocage après la saisie de plusieurs faux codes :

- Le blocage croissant :
  - Après 4 faux codes = 10' de blocage
  - Puis, si le code suivant est faux = 20' de blocage
  - Puis, pour chaque faux code saisi = 30' de blocage.
- Le blocage fixe ; La durée du blocage est paramétrable de 3 à 99 minutes en classe B ou C et de 8 à 99 minutes en classe D.

La saisie d'un bon code réinitialise le compteur de faux codes.

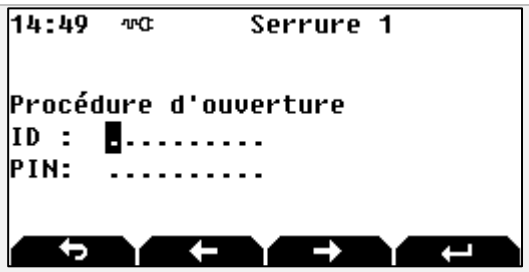
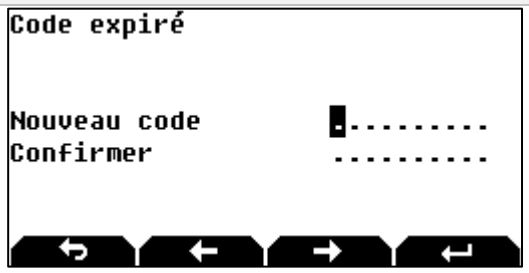
3.10 Messages

Les messages suivants peuvent apparaître lors du réveil de la serrure :

Message	Cause	Action
Trappe piles ouverte	La trappe d'accès aux piles est ouverte code est incorrect.	Refermer la trappe pile.
Anti-arrachement ouvert	L'anti-arrachement de l'Unité de saisie est activé.	Vérifier qu'il n'y a pas eu un démontage frauduleux de l'Unité de saisie. Remonter l'Unité de saisie sur son support.
L'anti-arrachement a été activé !	L'anti-arrachement de l'Unité de saisie a été activé.	Vérifier qu'il n'y a pas eu un démontage frauduleux de l'Unité de saisie.

3.11 Changement obligatoire du code lors de la première utilisation

Le système rend obligatoire ce changement de code uniquement pour les utilisateurs à partir de l'identifiant 4. Toutefois, à l'utilisation, il conviendra de ne pas laisser de code usine pour les identifiants 1 à 3.

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Utilisez les flèches ▼ et ▲ pour sélectionner **Procédure d'ouverture** ou **Accès au menu** + ENTER
3		Tapez votre identifiant + ENTER Tapez le code 00000000 + ENTER
4		Le message **Code expiré** apparaît. Tapez votre code + ENTER Confirmez votre code + ENTER Un code correct est constitué d'au moins 6 chiffres pour la classe B, 7 pour la classe C et 8 pour la classe D.

Le code doit être confidentiel et saisi exclusivement dans un environnement sécurisé. S'il est connu ou suspecté d'être connu d'une autre personne, il doit être impérativement remplacé par un nouveau code.

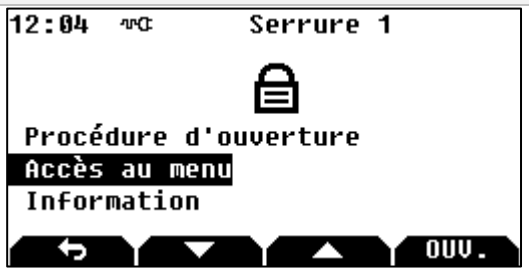
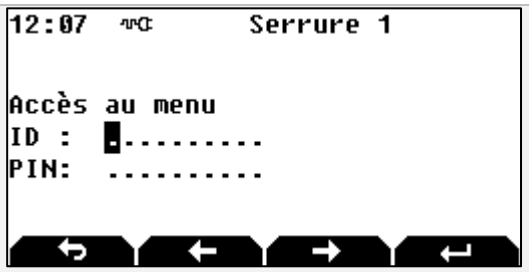
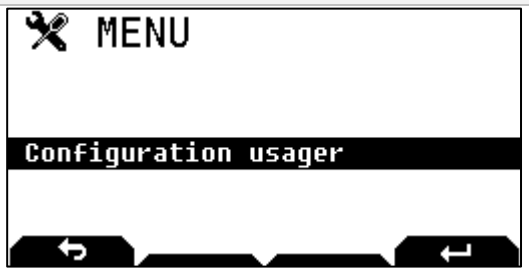
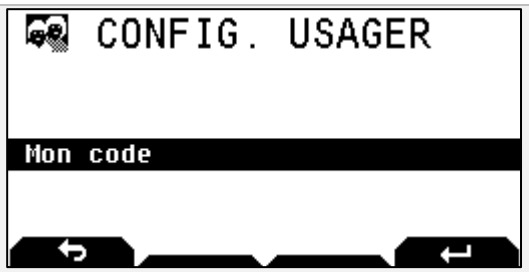
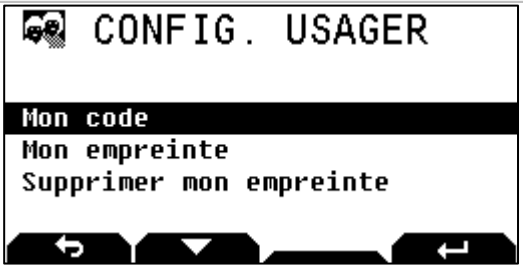
Ne pas utiliser :

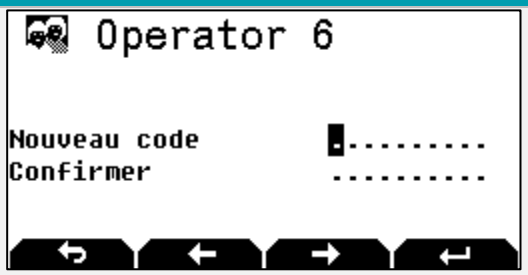
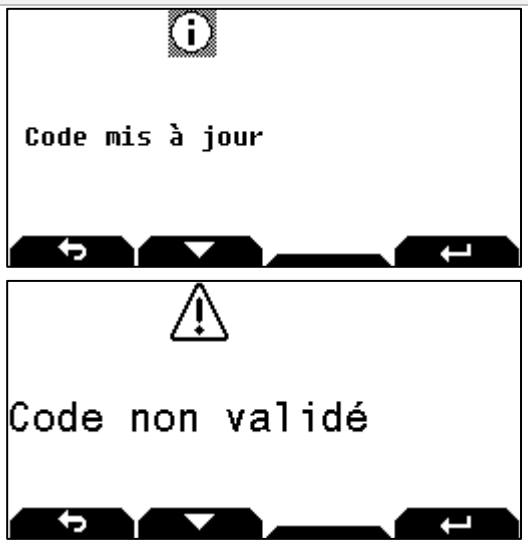
- **Les détails personnels (ex : date de naissance) ou toute autre donnée pouvant être reliée à l'utilisateur.**
- **Les codes triviaux : séries croissantes et décroissantes de digits (ex : 5-6-7-8-9-0-1-2 ou 3-2-1-0-9-8-7-6) ou séries de mêmes digits (ex : 4-4-4-4-4-4-4-4).**

Les pièces de la KeINet@ liées à la sécurité ne doivent pas être accessibles à des personnes non autorisées lorsque la porte du coffre auquel elle est fixée est ouverte.

Après un changement de code, la serrure doit être essayée plusieurs fois, la porte étant en position ouverte.

3.12 Changement du code à l'initiative de l'utilisateur

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▼ .
2		Utilisez la flèche ▼ pour sélectionner **Accès au menu** + ENTER
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER Dans le cas où un utilisateur doit s'identifier avec son empreinte, celle-ci lui sera demandée.
4		Appuyez sur ENTER Pour un utilisateur sans reconnaissance d'empreinte, passez à l'étape 5, sinon passez à l'étape **6**
5		Appuyez sur ENTER et passez à l'étape **7**.
6		Sélectionnez **Mon code** et appuyez sur ENTER .

Etape	Ecran	Description
7		Saisissez et confirmez votre nouveau code et appuyez sur ENTER.
8		Si l'affichage indique **Code mis à jour**, le code a été changé ; sinon, si l'affichage indique **Code non validé**, il faut reprendre à l'étape **4**.

Le code doit être confidentiel et saisi exclusivement dans un environnement sécurisé. S'il est connu ou suspecté d'être connu d'une autre personne, il doit être impérativement remplacé par un nouveau code.

Ne pas utiliser :

- **Les détails personnels (ex : date de naissance) ou toute autre donnée pouvant être reliée à l'utilisateur.**
- **Les codes triviaux : séries croissantes et décroissantes de digits (ex : 5-6-7-8-9-0-1-2 ou 3-2-1-0-9-8-7-6) ou séries de mêmes digits (ex : 4-4-4-4-4-4-4-4).**

Les pièces de la KeINet@ liées à la sécurité ne doivent pas être accessibles à des personnes non autorisées lorsque la porte du coffre auquel elle est fixée est ouverte.

Après un changement de code, la serrure doit être essayée plusieurs fois, la porte étant en position ouverte.

4 CONFIGURATION DE L'UNITE DE SAISIE

4.1 Configuration de base de l'Unité de saisie

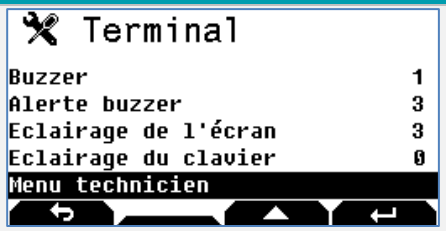
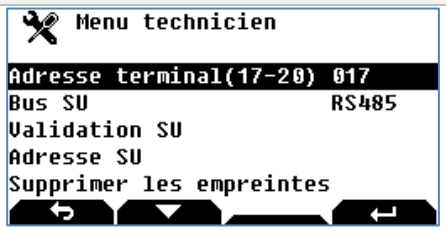
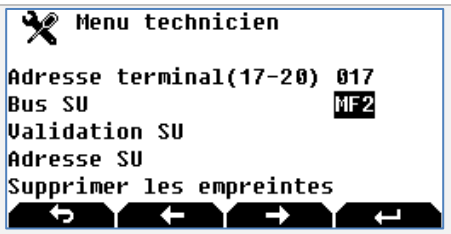
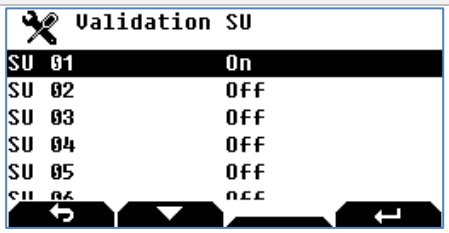
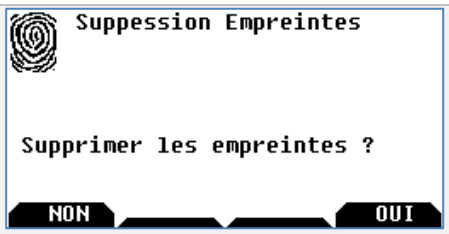
Etape	Ecran	Description
1		Sélectionnez le **Menu terminal** avec ▲ + ENTER
2		Réglage disponible dans le **Menu terminal**.

Pour retourner à l'écran précédent, appuyez sur ↩.

Fonction	Sous-fonction	Description
Terminal	Langue	Permet de choisir la langue des messages affichés par le terminal.
	Information	Permet d'afficher les informations du terminal
	Buzzer	Permet de régler le niveau sonore du buzzer pour l'appui sur une touche
	Alerte buzzer	Permet de régler le niveau sonore du buzzer en cas d'alarme
	Eclairage écran	Permet de sélectionner le niveau d'éclairage de l'écran
	Eclairage clavier	Permet de sélectionner le niveau d'éclairage du clavier

4.2 Configuration avancée (Menu technicien)

Le Menu technicien n'est visible que si le switch anti-arrachement de l'Unité de saisie est ouvert.

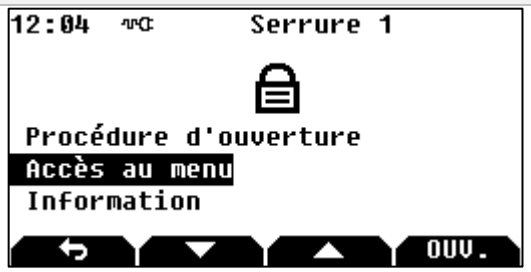
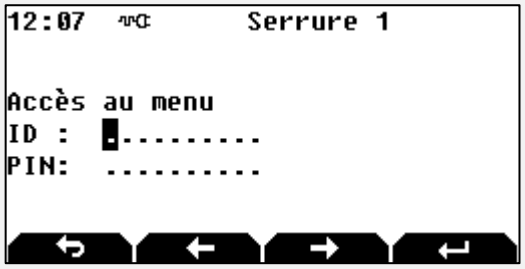
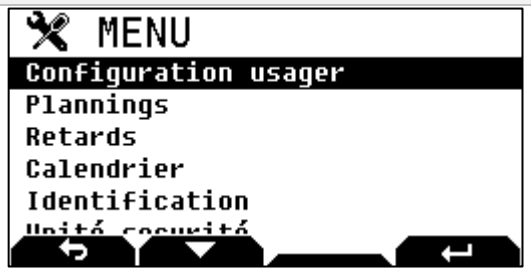
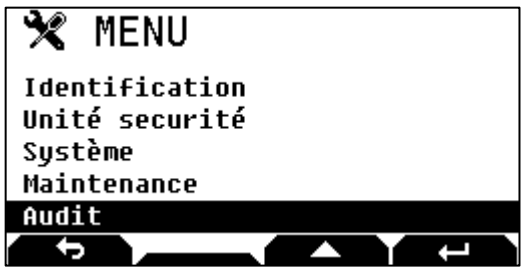
Etape	Ecran	Description
1		Sélectionnez le **Menu technicien** + ENTER.
2		Configuration l'adresse de l'Unité de saisie de 17 à 20. L'adresse 17 correspond à la 1ère Unité de saisie.
3		Le menu **Bus SU** permet de choisir le bus de communication avec les serrures : • Soit MF2 (par défaut) • Soit RS485 Le bus RS485 ne permet pas un fonctionnement sur batterie uniquement.
4		Le menu **Validation SU** permet de valider les serrures qui seront gérées par l'Unité de saisie. Mettre à **ON** les serrures valides.
5		Le menu **Suppression Empreintes** permet de supprimer toutes les empreintes du capteur d'empreinte monté sur l'Unité de saisie.

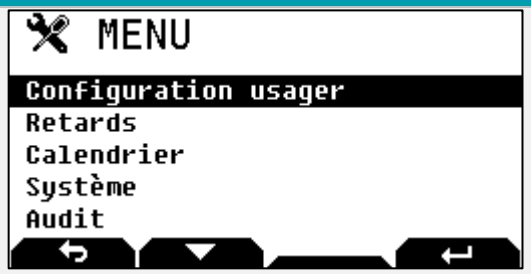
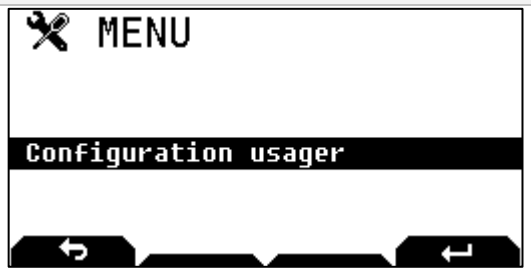
Tant que le switch anti-arrachement est ouvert, le message « **Anti-arrachement ouvert** » est affiché et seul l'accès au menu de l'Unité de saisie est autorisé.
Sinon, le message suivant apparait :

Ce message est affiché tant qu'il n'y a pas eu une identification valide, mais il ne bloque pas la serrure.

5 CONFIGURATION DE L'UNITE DE SECURITE

5.1 Accès au menu de configuration

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Utilisez la flèche ▼ pour sélectionner **Accès au menu** + ENTER
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER Dans le cas où un utilisateur doit s'identifier avec son empreinte, celle-ci lui sera demandée. Suivant la configuration de la serrure, il est possible que l'accès aux menus nécessite une procédure « 4 yeux » (identification de deux utilisateurs différents). Les menus disponibles sont affichés en fonction des droits : • Super Manager : étape **4** • Manager : étape **5** • Utilisateur : étape **6**
4	 	Menus disponibles pour un **Super Manager**

Etape	Ecran	Description
5		Menu disponible pour un **Manager**
6		Menu disponible pour un **Utilisateur**

Pour retourner à l'écran précédent, appuyez sur ↵.

Le contenu du menu est différent selon les droits de l'utilisateur.
Chaque utilisateur ne voit que les fonctions qu'il peut modifier.

5.2 Liste des menus

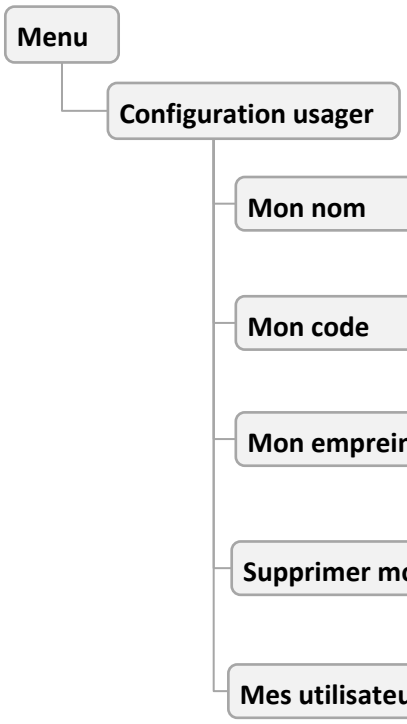
La liste du menu principal, selon les droits de l'utilisateur, contient une partie ou la totalité des fonctions suivantes (**SM** : Super Manager ; **M** : Manager ; **U** : Utilisateur) :

Fonction	Sous-fonction	Description	SM	M	U
Configuration usager	Mon nom	Permet de changer mon nom.	✓	✓	
	Mon code	Permet de changer mon code.	✓	✓	✓
	Mon empreinte(1)	Permet d'enregistrer mon empreinte digitale.	✓	✓	✓
	Supprimer mon empreinte(1)	Permet de supprimer mon empreinte digitale.	✓	✓	✓
	Mes utilisateurs	Permet d'activer ou de désactiver les utilisateurs sous ma responsabilité.	✓	✓	
Plannings	Planning standard	Permet de modifier un planning standard.	✓		
	Planning étendu	Permet de modifier un planning "étendu".	✓		
	Périodes étendues	Permet de définir les dates de périodes étendues.	✓		
Retards	Retard 1 à Retard 4	Après sélection d'un planning, permet de définir le retard à l'ouverture.	✓	✓	
	Retard 4 yeux	Après sélection d'un planning, permet de définir le retard à l'ouverture en mode "4 yeux".	✓	✓	
Calendrier	Jours fériés	Permet d'activer ou non un jour férié.	✓	✓	
	Fermeture exceptionnelle	Permet de définir les dates et heures des fermetures exceptionnelles.	✓	✓	
	Ouverture exceptionnelle	Permet de définir les dates et heures des ouvertures exceptionnelles.	✓	✓	
Identification	Suspension automatique	Après sélection d'un groupe de droits, permet de changer le nombre de jours au bout duquel un code devient inactif.	✓		
	Expiration du code	Après sélection d'un groupe de droits, permet de changer le nombre de jours au bout duquel un nouveau code doit être saisi.	✓		
	Anti retour	Après sélection d'un groupe de droits, permet de changer la méthode qui permet à un utilisateur de s'identifier une seconde fois.	✓		
	Retard fixe	Après sélection d'un groupe de droits, permet de forcer la valeur des retards en minutes à l'ouverture. Valeur = 255 si le retard est défini dans les plannings.	✓		
Unité sécurité	MID	Affiche le numéro MID (Module Identification) de l'Unité de Sécurité.	✓		
	Paramètres + Id après retard	Permet d'activer ou non la ré-identification après retard.	✓		
	Paramètres + Fermeture par Id	Permet d'activer ou non la fermeture par identification.	✓		
	Paramètres + Timeout pêne rentré	Permet de changer le temps du timeout au bout duquel la serrure se referme.	✓		
	Paramètres + Blocage après ferm.	Permet de changer le temps de blocage d'une nouvelle ouverture après une procédure de fermeture (en minute).	✓		
	Paramètres + Temps autorisation accès(G1)	Permet de changer le temps d'autorisation d'accès (procédure G1), valeur = 15 à 180 secondes. Si la valeur est 0, la fonction « Autorisation d'accès G1 » n'est pas activée.	✓		
	Paramètres + Digit alarme	Permet de saisir une valeur ajoutée au code pour déclencher une alarme sous contrainte.	✓		
	Paramètres + Vitesse moteur	Permet de choisir une vitesse de rotation pour le moteur.	✓		
	Paramètres + Heure de fermeture 1	Permet de définir une heure de fermeture de la serrure. 00 :00 = pas d'heure de fermeture.	✓		
	Paramètres + Heure de fermeture 2	Permet de définir une seconde heure de fermeture de la serrure. 00 :00 = pas d'heure de fermeture.	✓		

Fonction	Sous-fonction	Description	SM	M	U
	Entrées + I1, I2, O1/I5, O2/I6, IL, BP	Permet de choisir une fonction associée à l'entrée sélectionnée.	✓		
	Sorties + O1/I5, O2/I6, Relay, IL, Rouge, Vert	Permet de choisir une fonction associée à la sortie sélectionnée.	✓		
Système	Réglage horloge	Permet d'ajuster la date et l'heure.	✓	✓	
	Heure été/hiver	Permet d'activer ou non le changement d'heure automatique été / hiver.	✓		
	Mode parallèle	Permet d'activer ou non le mode parallèle.	✓		
	Asservissement	Permet de choisir une règle d'asservissement.	✓		
Maintenance	Accès au téléchargement	Permet d'autoriser le téléchargement de la configuration d'une Unité de Sécurité ou de faire une mise à jour firmware via l'Outil de Configuration.	✓		
	Sécurisation + Sécuriser la liaison IU-SU	Permet de lancer la procédure de sécurisation de la liaison Unité de saisie/Unité de Sécurité.	✓		
	Sécurisation + Autoriser la sécurisation par CT	Autorise la sécurisation de tous les périphériques du site par le CT.	✓		
	Clé USB + Ecriture configuration (CT -> US)	Permet de charger dans la serrure, à l'aide d'une clé USB, une configuration préalablement réalisée avec l'Outil de Configuration.	✓		
	Clé USB + Lecture configuration (US -> CT)	Permet de récupérer, sur une clé USB, la configuration de la serrure pour l'exploiter ensuite par l'Outil de Configuration.	✓		
	Clé USB + Ecriture planning (CT -> US)	Permet de charger dans la serrure, à l'aide d'une clé USB, les plannings préalablement réalisés avec l'Outil de Configuration.	✓		
	Clé USB + Lecture planning (US -> CT)	Permet de récupérer, sur une clé USB, les plannings de la serrure pour l'exploiter ensuite par l'Outil de Configuration.	✓		
	Mode OTC	Permet d'activer le mode OTC désiré : Désactivé, OTC standard, OTC via IP	✓		
	Clé OTC	Permet de configurer la clé du mode OTC.	✓		
	Accès au menu	Permet de sélectionner le type d'identification pour accéder au menu.	✓		
Audit	Afficher l'audit	Pour afficher les évènements passés sur l'Unité de saisie.	✓	✓	
	Charger l'audit sur une clé USB	Pour sauvegarder les évènements passés sur une clé USB.	✓	✓	
	Afficher l'audit des téléch pro	Afficher l'historique de mise à jour du logiciel	✓	✓	

(1) Uniquement pour les usagers dont le mode d'identification est « Code PIN + Empreinte ».

5.3 Configuration des paramètres utilisateur



Entrez le nom de l'utilisateur avec le clavier + ENTER.

Entrez le nouveau code de l'utilisateur avec le clavier et confirmez-le ENTER.

Modifiez l'empreinte digitale de l'utilisateur.
L'empreinte est effacée dès le début de la procédure. Si la procédure est interrompue, il faudra recommencer.

Supprimez l'empreinte digitale de l'utilisateur + ENTER.

Accès aux paramètres de ses utilisateurs + ENTER.
L'écran affiche la liste des utilisateurs sur lesquels on a les droits.
Fonctions disponibles (en fonction des droits) :

- **Nom de l'utilisateur** : Changer le nom de l'utilisateur
- **Etat de validation (On/Off)** : Activer ou désactiver manuellement le droit de l'utilisateur à ouvrir la serrure
- **Blocage anti-retour (On/Off)** : Activer ou désactiver le blocage anti-retour
- **Période d'activation** : Activer ou désactiver le droit de l'utilisateur à ouvrir la serrure
    - Début
    - Fin
- **Changement de code** : Modification du code d'ouverture de l'utilisateur

** Uniquement pour les usagers dont le mode d'identification est « Code PIN + Empreinte »*

Les différents paramètres sont accessibles en fonction des droits de l'utilisateur concerné.

Les paramètres de l'utilisateur sont changés uniquement dans l'Unité de Sécurité sélectionnée avant d'entrer dans le menu.
Répétez la même opération pour changer les paramètres dans les autres Unités de Sécurité.

5.4 Configuration des plannings

Menu

Plannings

Schedule 1

Semaine standard

Cette définition de semaine est utilisée pour les jours **hors périodes étendues**.

- Choisissez une journée.
- Sélectionnez une plage horaire.
- Réglez l'heure de début et le mode de fonctionnement.

Semaine étendue

Cette définition de semaine est utilisée pour les **jours des périodes étendues**.

- Choisissez une journée.
- Sélectionnez une plage horaire.
- Réglez l'heure de début et le mode de fonctionnement.

Périodes étendues

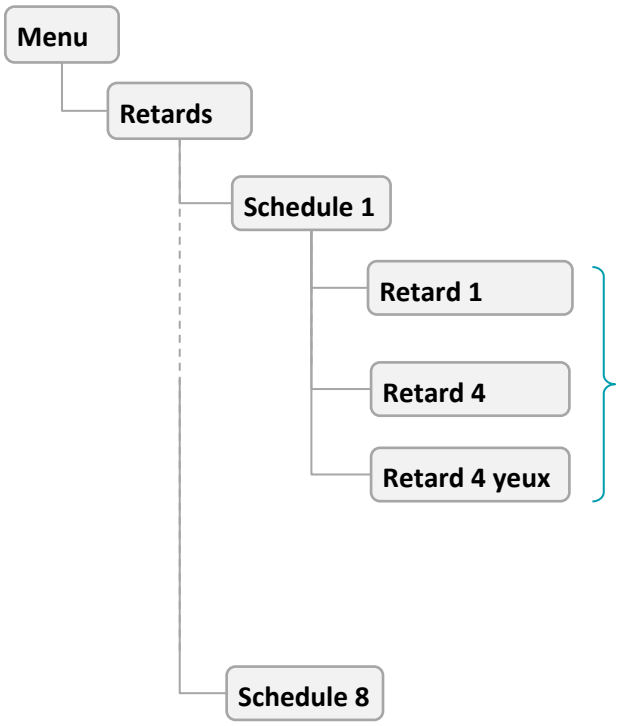
Pendant une **période étendue**, le planning de la **semaine étendue** est appliqué.

- Choisissez une des 5 périodes possibles.
- Réglez la date de début et la date de fin.

Schedule 8

Les 8 plannings possèdent les mêmes possibilités de réglage.
La définition d'une journée peut être copiée vers une autre journée, avec la fonction copie en bas de la liste des jours :

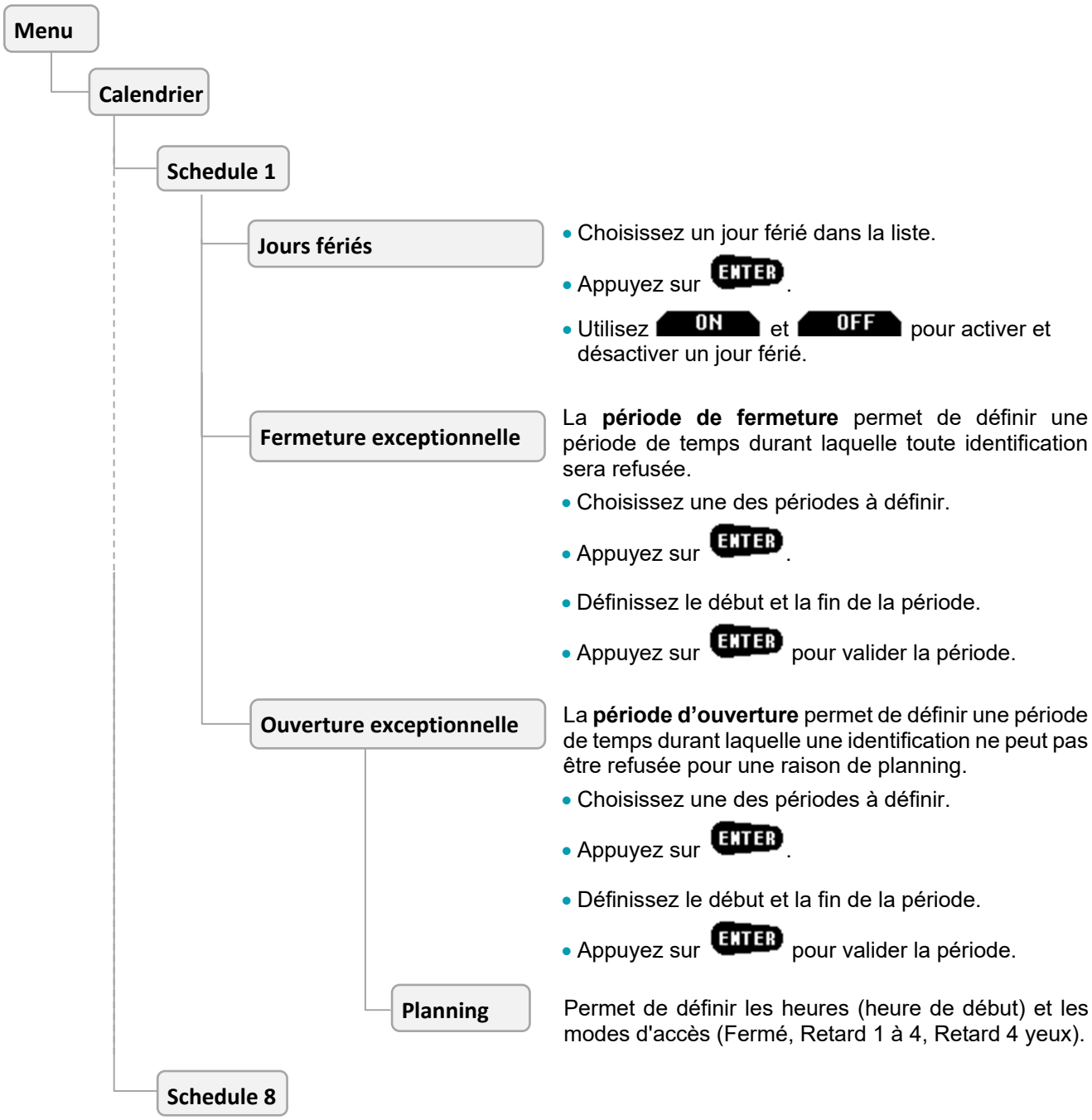
5.5 Configuration des retards



- Choisissez un retard.
- Appuyez sur ENTER.
- Réglez sa valeur, en minutes, avec le clavier.
- Validez avec ENTER.

Les 8 Plannings possèdent les mêmes possibilités de réglage.

5.6 Configuration du calendrier



- Choisissez un jour férié dans la liste.
- Appuyez sur ENTER.
- Utilisez ON et OFF pour activer et désactiver un jour férié.

La **période de fermeture** permet de définir une période de temps durant laquelle toute identification sera refusée.

- Choisissez une des périodes à définir.
- Appuyez sur ENTER.
- Définissez le début et la fin de la période.
- Appuyez sur ENTER pour valider la période.

La **période d'ouverture** permet de définir une période de temps durant laquelle une identification ne peut pas être refusée pour une raison de planning.

- Choisissez une des périodes à définir.
- Appuyez sur ENTER.
- Définissez le début et la fin de la période.
- Appuyez sur ENTER pour valider la période.

Permet de définir les heures (heure de début) et les modes d'accès (Fermé, Retard 1 à 4, Retard 4 yeux).

Les 8 plannings possèdent les mêmes possibilités de réglage.

5.7 Configuration de l'identification

Menu

Identification Choisissez le groupe de droits désiré et appuyez sur ENTER.

Manager 1

Suspension auto. Appuyez sur ENTER et saisissez le nombre de jours au bout duquel un code est suspendu s'il n'est pas utilisé.

Expiration du code Appuyez sur ENTER et saisissez le nombre de jours au bout duquel un nouveau code sera demandé.

Anti retour Appuyez sur ENTER et définissez le mode d'anti-retour.

Le mode anti-retour définit les conditions qui autorisent un utilisateur déjà identifié à pouvoir s'identifier une seconde fois :

- **Désactivé** : pas de blocage sur une seconde identification.
- **Manuel** : Réactivation manuelle sur l'Unité de saisie.
- **Id correct** : Réactivation par une identification correcte d'un autre utilisateur.
- **Autre groupe** : Réactivation par une identification correcte d'un utilisateur d'un autre groupe de droits.
- **Procédure CIT** : Réactivation par une identification correcte d'un utilisateur d'un autre groupe de droits.

€ est affiché à la fin de la procédure CIT

Retard fixe Appuyez sur CLEAR et définissez la durée du retard (en minutes) à l'ouverture pour ce groupe de droits.

Valeur = 255 si le retard est défini dans les plannings.

Manager 2

Manager CIT

Operator CIT

Operator

Super Manager

Code + fp

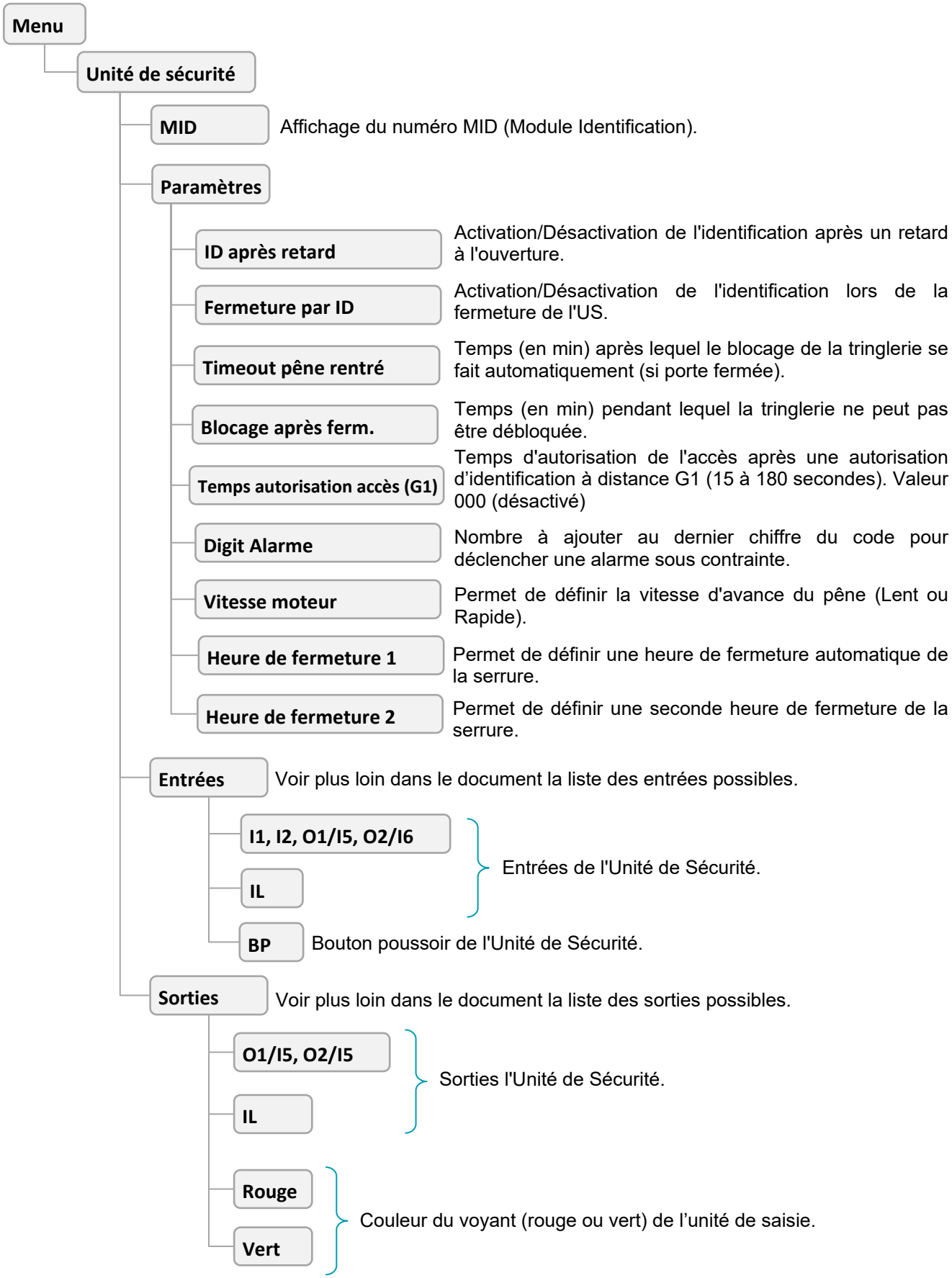
OTC

Mêmes paramètres que **Manager 1**

Les 8 groupes possèdent les mêmes possibilités de réglage.

Lors de l'utilisation de codes à usage unique (OTC), le logiciel d'application générant les codes à usage unique ne doit être installé que dans un environnement sécurisé.

5.8 Configuration de l'Unité de Sécurité



Liste des fonctions des entrées

N	Fonction
1	**Commande d'ouverture** Commande directe de l'ouverture (uniquement si la serrure n'est pas certifiée).
2	**Contact tringlerie** Cette entrée est activée lorsque la porte est ouverte. L'unité de saisie affichera alors :  .
3	**Entrée signal alarme** Entrée d'un signal alarme, par exemple alarme DOCT (Détection d'Ouverture Choc et Thermique).
4	**G1-Autorisation d'accès** Cette fonction n'est possible que si le temps « Autorisation d'accès (G1) » a une valeur comprise entre 15 à 180 secondes. Lorsque l'entrée est désactivée, les accès sont bloqués. Lorsque l'entrée est activée (et pendant 2 minutes après la désactivation), les accès sont autorisés. Cette fonction s'applique à l'ouverture et à l'accès aux menus par l'Unité de saisie. **Attention à l'utilisation de la procédure G1 car celle-ci peut bloquer une serrure si la commande d'autorisation G1 ne fonctionne pas.**
5	**G2-Ouverture sans retard** Lorsque l'entrée est activée (et pendant 2 minutes après la désactivation), l'ouverture se fait sans retard.
6	**G3-Annulation ouverture** Lorsque l'entrée est activée, le délai en cours est annulé et l'ouverture est impossible.
7	**G4-Retard de substitution** Lorsque l'entrée est activée (et pendant 2 minutes après la désactivation), l'ouverture se fait avec le retard de substitution.
8	**Bouton déporté ALSC (alarme sous contrainte)** L'alarme sous contrainte est activée si le bouton déporté n'est pas appuyé durant le retard. Plus précisément, le bouton doit être activé : ○ après 5 secondes après le début du retard ○ avant 5 secondes avant la fin du retard.
9	**Suspension d'ouverture** Si cette entrée est activée, en fin de décompte du retard : ○ L'unité de saisie affiche pour cet ouvrant :  ○ La rentrée du pêne du moto verrou est suspendue. ○ La recomposition de code est également suspendue. Dès que l'entrée change d'état, la procédure d'ouverture peut reprendre.
10	**Ni retard - ni planning** Lorsque cette entrée est activée, l'ouverture ne tient pas compte des plannings et le délai avant ouverture est nul.
11	**Entrée asservissement** Lorsque cette entrée est activée, l'ouverture est interdite.

Par défaut, toutes les entrées sont ouvertes au repos.

Liste des fonctions des sorties

N	Fonction
1	**Pêne entièrement rentré** Cette sortie est activée lorsque le pêne est complétement rentré.
2	**Gestion alarme externe** Cette sortie est activée lorsque la serrure est déverrouillée. Cette sortie permet par exemple de couper une alarme DOCT.
3	**Identification correcte** Cette sortie est activée pendant 3 secondes après une bonne identification (ouverture ou accès menu).
4	**Retard en cours** Cette sortie est activée pendant toute la durée du délai avant ouverture.
5	**Fin du retard** Cette sortie est activée à la fin du délai et : • pendant la durée d'attente du second code • ou pendant l'attente s'il y a suspension d'ouverture • ou pendant l'asservissement si celui-ci est actif
6	**Alarme sous contrainte** Cette sortie est activée lorsqu'il y a une alarme sous contrainte et pendant un temps paramétrable, par défaut 3 secondes.
7	**Alarme pêne bloqué** Cette sortie est activée dès qu'il y a un défaut de verrouillage ou de déverrouillage.
8	**Porte ouverte trop longtemps** La sortie est activée lorsque la porte est ouverte trop longtemps. Ce temps est défini par le paramètre « **Durée d'ouverture de la porte** » ajouté au temps « **Alerte après la durée d'ouverture de la porte** ».
9	**Sortie signal alarme** Cette sortie suit l'état de l' « **Entrée signal alarme** » sauf pendant les mouvements du pêne et lorsque la porte est déverrouillée. La sortie est maintenue pendant 20 secondes après disparition du signal d'entrée.
10	**Blocage code faux** Cette sortie est activée lorsqu'il y a eu plus de 3 mauvaises identifications. La sortie est désactivée lorsqu'il y a une bonne identification.
11	**Blocage horaire** La sortie est activée lorsque tous les usagers sont bloqués (soit par des plages horaires, soit par des jours fériés ou des fermetures exceptionnelles.
12	**Commande déverrouillage** = fonction relais déporté Cette sortie est activée si l'ouverture a été réalisée par un usager qui a le « **Droit de commander la sortie télécommandée** ». La sortie est désactivée lorsque la serrure est à nouveau verrouillée.
13	**Alerte sonore** La sortie est activée lorsque la porte est ouverte trop longtemps. Ce temps est défini par le paramètre « **Durée d'ouverture de la porte** ». La sortie est désactivée dès que la porte est refermée. Le temps maximum d'activation de cette sortie est défini par le paramètre « **Alerte après la durée d'ouverture de la porte** ».
14	*Réservé*
15	**Alarme coupure alim.** La sortie est activée après une coupure d'alimentation. La sortie est désactivée lors de la prochaine bonne identification.

N	Fonction
16	*Réservé*
17	*Réservé*
18	**Sortie asservissement** Cette sortie est activée lorsque la serrure n'est pas verrouillée.
19	**Niveau batterie faible** Cette sortie est activée lorsque le niveau de batterie est inférieur à 6,3V.
20	**Alimentation externe OK** Cette sortie est activée lorsque la tension alimentation est supérieure à 11V
21	**Accès refusé (G1)** La sortie est activée tant qu'il n'y a pas une autorisation d'accès par la procédure G1.

Par défaut, l'état des sorties est « non activée au repos ».

5.9 Configuration du système

Réglage horloge

Appuyez sur ENTER et modifiez la date et l'heure dans une limite de +/- 75 min.

Un usager ayant des droits d'installation ou d'administration n'est pas concerné par cette limitation.

Heure été/hiver

Appuyez sur ENTER et sélectionnez le mode de changement d'heure automatique :

Off : Désactivé
1 : Dernier dimanche de mars et dernier dimanche d'octobre
2 : Second dimanche de mars et premier dimanche de novembre
3 : Second dimanche de mars et dernier dimanche d'octobre
4 : Premier dimanche d'avril et premier dimanche d'octobre
5 : Troisième dimanche de février et troisième dimanche d'octobre

Mode parallèle

Appuyez sur ENTER et activez ou désactivez le mode parallèle avec ON et OFF.

Un utilisateur ne pourra ouvrir qu'une seule serrure à la fois. Si 2 serrures sont montées sur la même porte, il faudra 2 utilisateurs différents.

Asservissement

Appuyez sur ENTER et choisissez un des modes suivants :

- **Désactivé** : pas d'asservissement.
- **Règle 1** : si une procédure d'ouverture est en cours, il n'est pas possible d'ouvrir une autre serrure ou même lancer un autre retard.
- **Règle 2** = « retard une fois » :
  La première ouverture est réalisée avec le délai normal.
  Pendant le délai et pendant l'ouverture, on ne peut pas ouvrir les autres serrures.
  Lorsque la serrure est verrouillée, dans les 2 minutes qui suivent, on peut ouvrir celle-ci ou une autre SU sans délai.

5.10 Maintenance

Appuyez sur ENTER pour autoriser le téléchargement de données à partir du PC (par USB ou IP) dans l'Unité de Sécurité pendant 1 heure.

Appuyez sur ENTER et choisissez la liaison à sécuriser :

- **Sécuriser la liaison IU-SU**
- **Autoriser la sécurisation par CT**

Voir §8. SECURISATION.

Appuyez sur ENTER et mettez à jour ou sauvegardez la configuration ou les plannings.

Suivez les instructions à l'écran et attendez la fin des transferts.

Voir §6. « MODIFICATION DE LA CONFIGURATION PAR CLE USB ».

Appuyez sur ENTER et choisissez un des modes suivants :

- **Désactivé**
- **OTC standard**
- **OTC via IP**

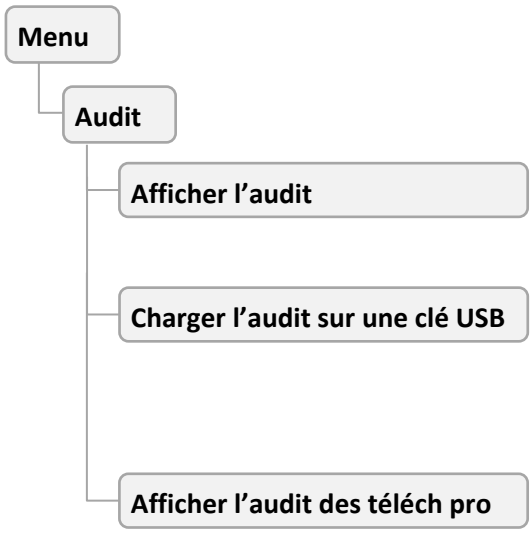
Appuyez sur ENTER, définissez et confirmez la clé OTC de 20 chiffres.

Appuyez sur ENTER et choisissez un des modes suivants :

- **2 yeux**
- **4 yeux, droits restreints**
- **4 yeux, droits du dernier usager**
- **OTC seulement**
- **Clé USB**

Lors de l'utilisation de codes à usage unique (OTC), le logiciel d'application générant les codes à usage unique ne doit être installé que dans un environnement sécurisé.

5.11 Audit



Appuyez sur ENTER pour afficher les évènements à l'écran.

Appuyez sur ENTER pour transférer les évènements sur une clé USB.
Suivez les instructions à l'écran et attendez la fin des transferts.

Appuyez sur ENTER pour afficher l'historique de mise à jour du logiciel.

Une clé USB peut être utilisée pour télécharger plusieurs journaux d'évènements de différentes serrures.

Utilisez uniquement des clés USB formatées avec un système de fichiers FAT32.

6 MODIFICATION DE LA CONFIGURATION PAR CLE USB

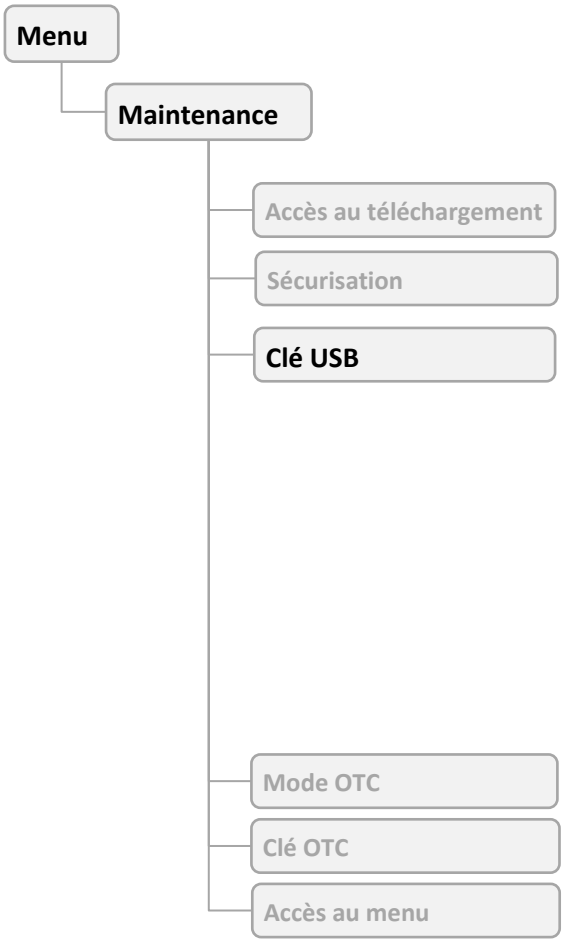
6.1 Introduction

Il est possible de modifier la configuration de la serrure KeINet@ à l'aide d'une clé USB sur laquelle une nouvelle configuration aura préalablement été enregistrée par l'Outil de Configuration.

De même, il est possible de récupérer les informations de configuration de la serrure pour les gérer dans l'Outil de Configuration (CT) sur PC.

6.2 Mise à jour de la configuration par clé USB

Pour accéder aux menus USB, l'utilisateur doit disposer des droits de gestion de la configuration par clé USB.



Cette procédure permet de mettre à jour la configuration de la serrure avec le contenu de la clé USB généré par l'Outil de Configuration.

- Ouvrez la trappe pile.
- Insérez la clé USB + ENTER.
- Choisissez **Ecriture configuration** + ENTER.
- Attendez la fin des étapes avec l'état d'avancement.
- Retirez la clé USB.
- Fermez la trappe pile.

La prise en compte de la nouvelle configuration est immédiate.

6.3 Lecture de la configuration et sauvegarde sur clé USB

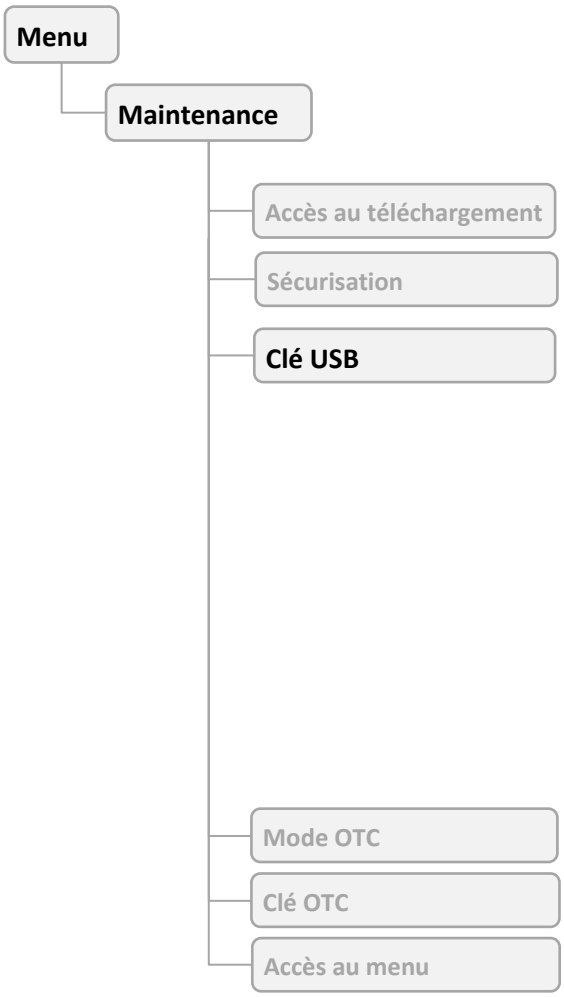
Pour accéder aux menus USB, l'utilisateur doit disposer des droits de gestion de la configuration par clé USB.

Cette procédure permet de récupérer la configuration de la serrure avec une clé USB pour être exploitée par l'Outil de Configuration.

- Ouvrez la trappe pile.
- Insérez la clé USB + ENTER.
- Choisissez **Lecture configuration** + ENTER.
- Attendez la fin des étapes avec l'état d'avancement.
- Retirez la clé USB.
- Fermez la trappe pile.

6.4 Mise à jour des plannings par clé USB

Pour accéder aux menus USB, l'utilisateur doit disposer des droits de gestion de la configuration par clé USB.

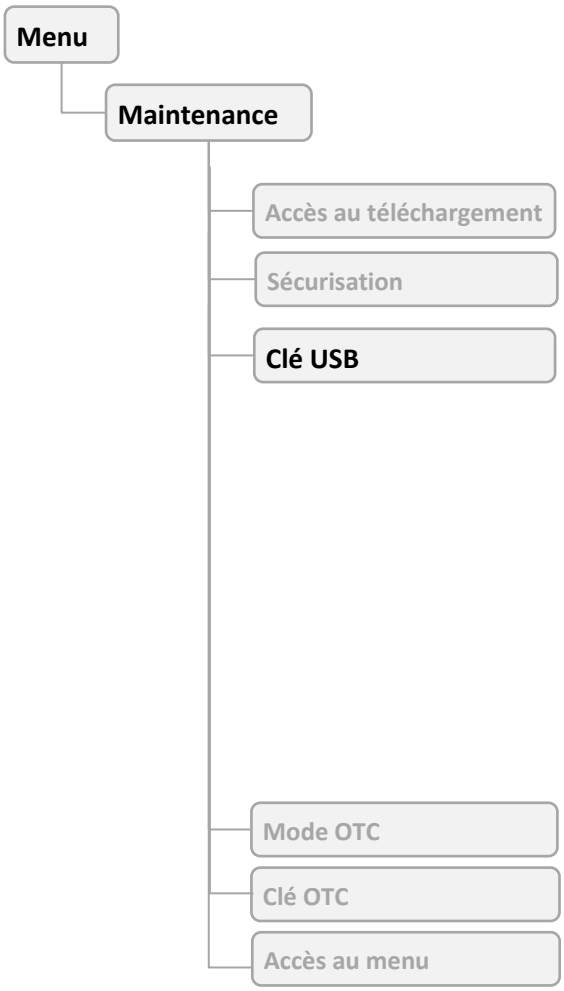


Cette procédure permet de mettre à jour les plannings de la serrure avec le contenu de la clé USB généré par l'Outil de Configuration.

- Ouvrez la trappe pile.
- Insérez la clé USB + ENTER.
- Choisissez **Ecriture planning** + ENTER.
- Attendez la fin des étapes avec l'état d'avancement.
- Retirez la clé USB.
- Fermez la trappe pile.

6.5 Lecture des plannings et sauvegarde sur clé USB

Pour accéder aux menus USB, l'utilisateur doit disposer des droits de gestion de la configuration par clé USB.



Cette procédure permet de récupérer les plannings de la serrure avec une clé USB pour être exploitée par l'Outil de Configuration.

- Ouvrez la trappe pile.
- Insérez la clé USB + ENTER.
- Choisissez **Lecture planning** + ENTER.
- Attendez la fin des étapes avec l'état d'avancement.
- Retirez la clé USB.
- Fermez la trappe pile.

7 EMPREINTE DIGITALE

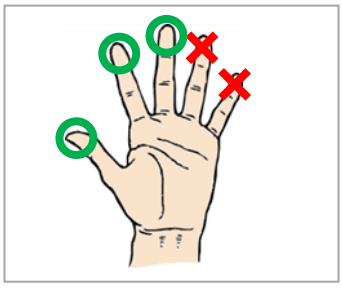
L'identification par empreinte digitale est toujours associée à un code.

L'enregistrement biométrique impose l'enregistrement de deux doigts différents.

Lors de l'installation d'une Unité de saisie, il est important de faire une suppression de toutes les empreintes via le **Menu technicien** (voir §4.2). Ceci permet d'initialiser la biométrie.

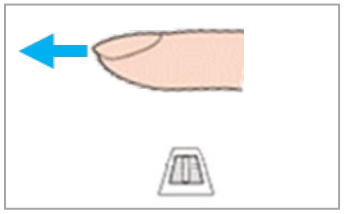
Seuls 25 utilisateurs peuvent être configurés en mode empreinte digitale.

7.1 Consignes pour l'enregistrement et la lecture d'empreintes

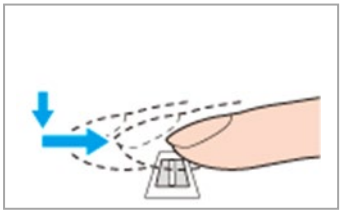


- Pour garantir un meilleur taux de réussite à l'enregistrement et à la lecture, évitez d'utiliser les plus petits doigts (auriculaire/annulaire).
- Ne soulevez pas votre doigt du capteur biométrique lors du passage.
- L'enregistrement ou la lecture de l'empreinte digitale peut échouer si vous bougez votre doigt trop rapidement ou trop lentement.
- Evitez toute torsion ou rotation du doigt lors du passage sur le capteur.
- Placement du doigt pour un fonctionnement optimal :

1. Insérez le doigt jusqu'à arriver en butée sans toucher le capteur biométrique.



2. Exercez une pression régulière sur le capteur biométrique en faisant glisser le doigt vers l'extérieur.



7.2 Enregistrement en mode « Code + Empreinte digitale »

Dans ce mode, l'utilisateur peut enregistrer son empreinte lui-même.

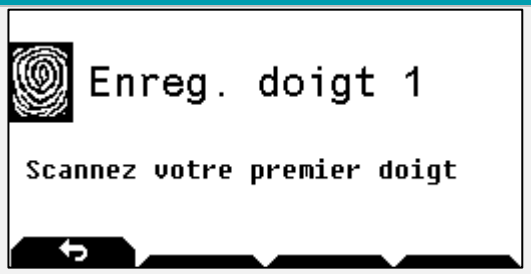
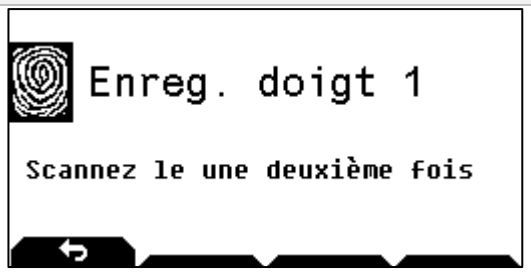
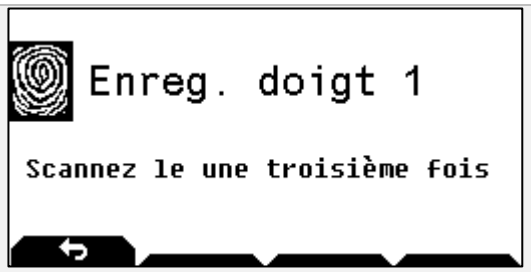
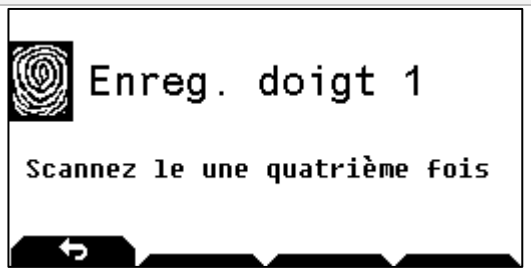
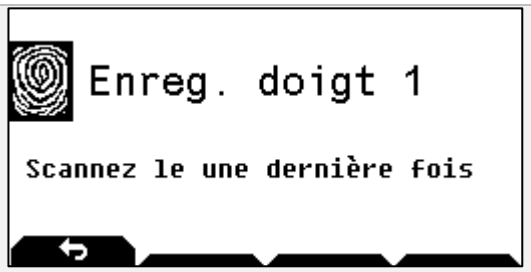
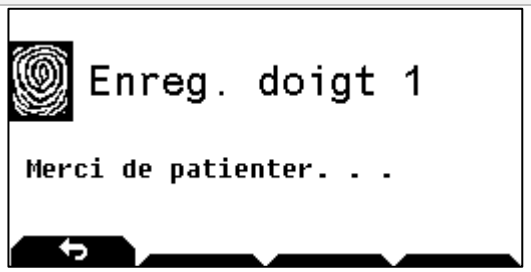
Cette procédure est faite automatiquement lors de la première procédure d'accès :

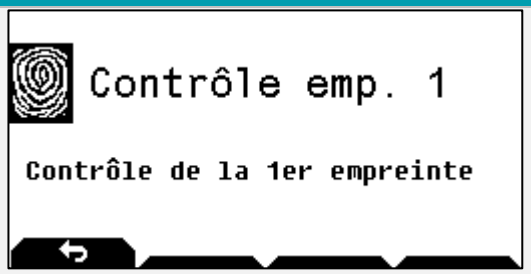
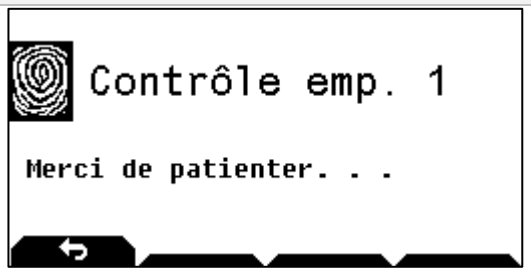
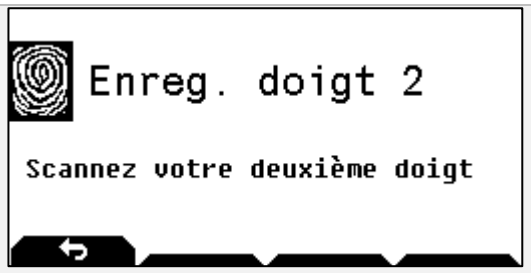
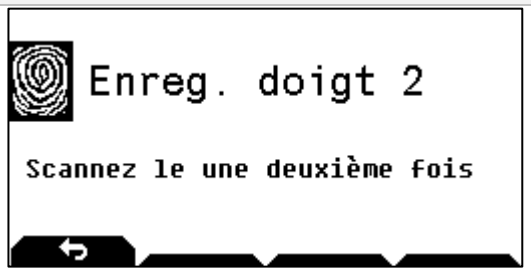
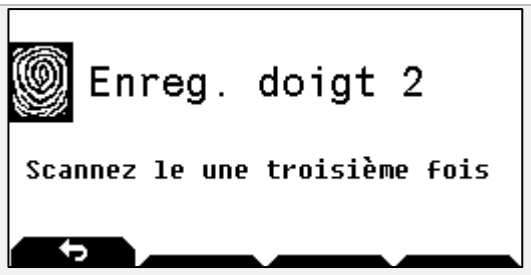
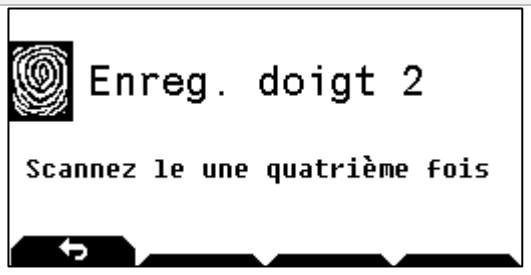
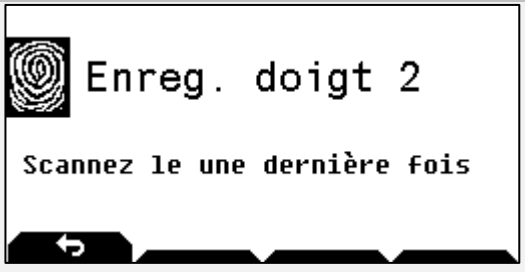
1. Sélectionnez l'Unité de Sécurité + ENTER.
2. Tapez votre identifiant + ENTER.
3. Tapez votre code PIN + ENTER.
4. Si ce code est utilisé pour la première fois, vous êtes invités à le modifier (voir § 3.11), puis à refaire une procédure d'accès en entrant votre nouveau code.
5. La procédure d'enregistrement commence (voir §7.3).

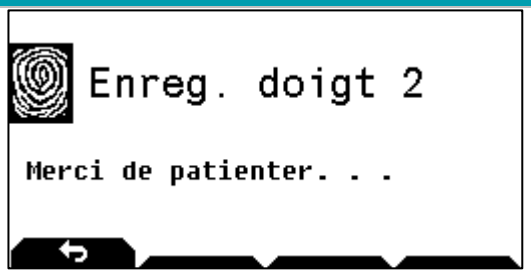
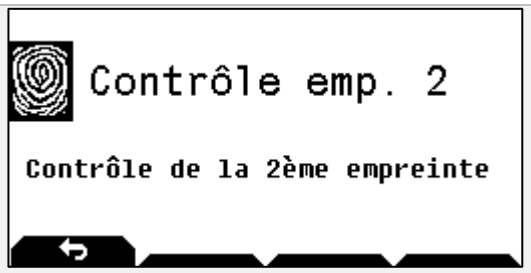
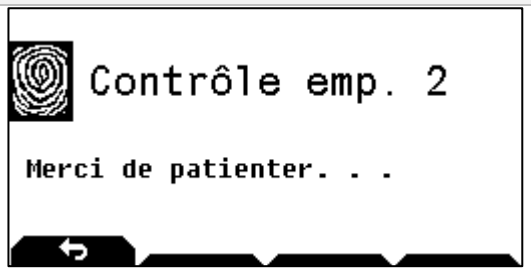
7.3 Procédure d'enregistrement

L'enregistrement d'une empreinte se fait en deux temps :

1. 5 lectures successives de la même empreinte pour en créer une image.
2. Vérification de l'image créée avec un contrôle de l'empreinte.

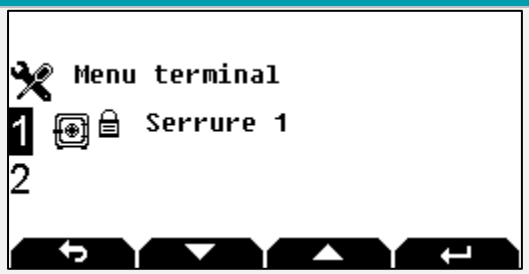
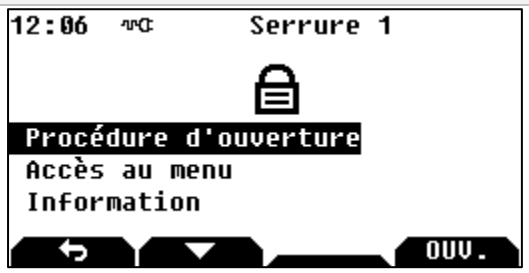
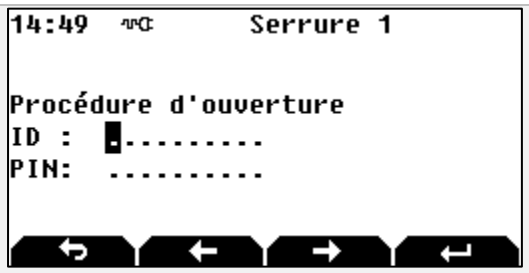
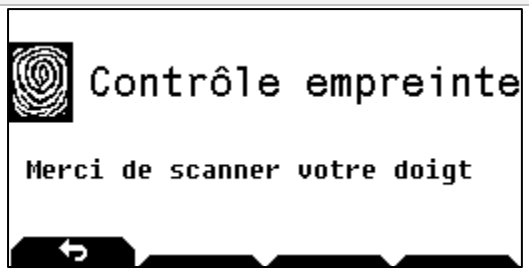
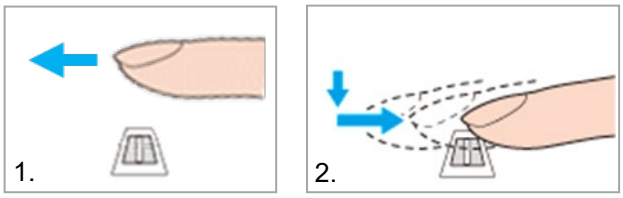
Etape	Ecran	Description
1		Passez une première fois votre premier doigt
2		Passez encore une deuxième fois votre premier doigt
3		Passez encore une troisième fois votre premier doigt
4		Passez encore une quatrième fois votre premier doigt
5		Passez une dernière fois votre premier doigt
6		Patientez pendant la création et la sauvegarde de l'empreinte

Etape	Ecran	Description
7		Passez votre premier doigt pour la vérification de la première empreinte.
8		Patientez pendant la vérification.
9		Passez une première fois votre deuxième doigt
10		Passez une deuxième fois votre deuxième doigt
11		Passez une troisième fois votre deuxième doigt
12		Passez une quatrième fois votre deuxième doigt
13		Passez une dernière fois votre deuxième doigt

Etape	Ecran	Description
14		Patientez pendant la création et la sauvegarde de l'empreinte
15		Passez votre deuxième doigt pour la vérification de la deuxième empreinte.
16		Patientez pendant la vérification.

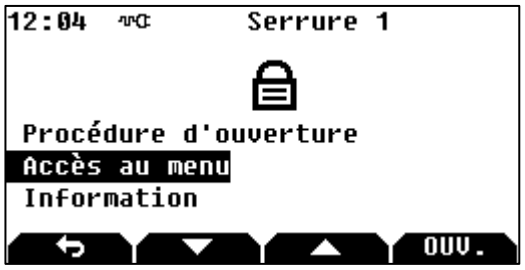
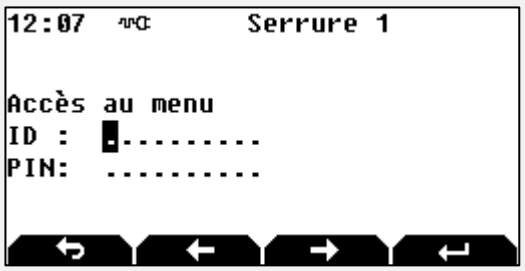
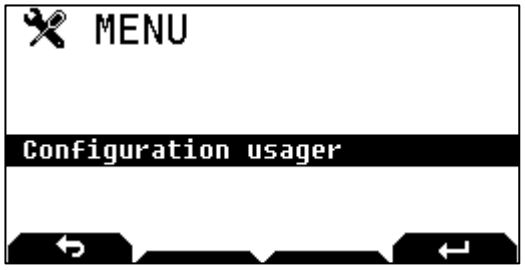
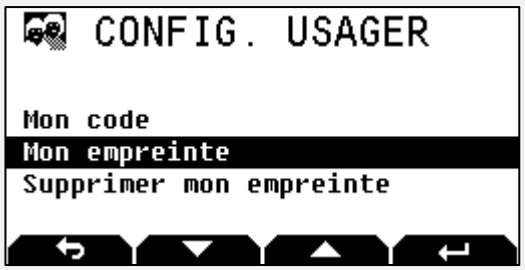
S'il y a plusieurs Unités de saisie sur le site, il faut réaliser l'enrôlement sur chaque Unité de saisie.

7.4 Procédure d'ouverture avec empreinte digitale

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▼ ..
2		Appuyez sur ENTER ou sur le bouton OUV. pour lancer la procédure d'ouverture.
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER
4		Glissez votre doigt sur le capteur biométrique. 
5		Patientez pendant le contrôle avec l'empreinte enregistrée. Si l'empreinte est correcte, la procédure continue normalement (ouverture du pêne, début retard, …).
6		Message d'erreur si l'empreinte n'est pas correcte.

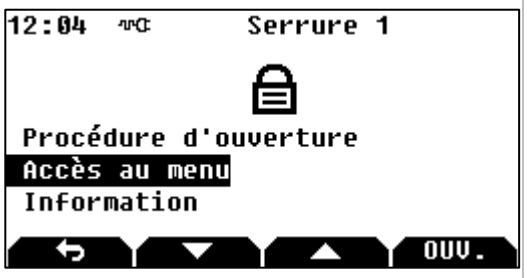
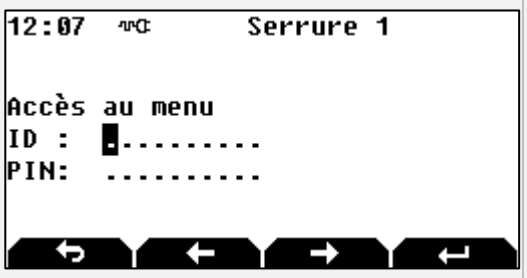
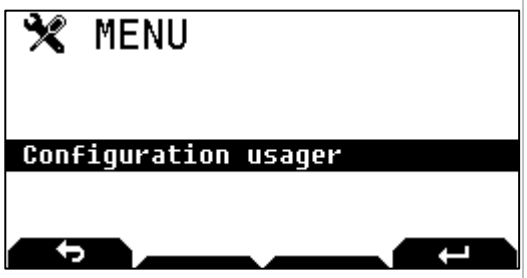
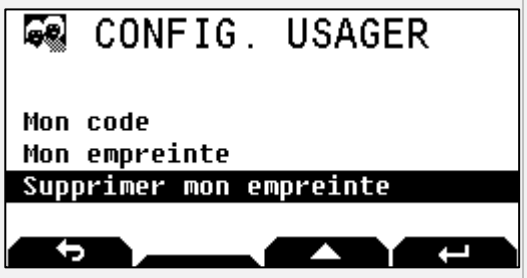
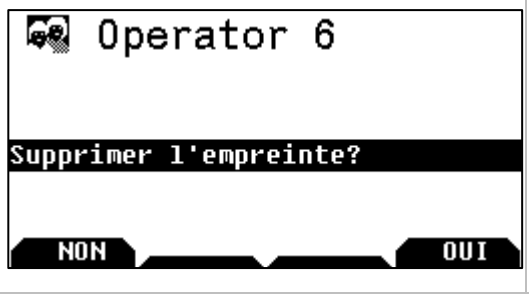
L'identification par empreinte peut aussi être utilisée pour accéder au menu.

7.5 Changement de l'empreinte à l'initiative de l'utilisateur

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour sélectionner une autre serrure, utilisez les flèches ▼ et ▲ .
2		Utilisez la flèche ▼ pour sélectionner **Accès au menu** + ENTER
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER Suivez les instructions pour le contrôle de l'empreinte.
4		Appuyez sur ENTER
5		Utilisez la flèche ▼ pour sélectionner **Mon empreinte** + ENTER . Suivez la procédure d'enregistrement d'une empreinte (cf. chapitre "Empreinte digitale").

S'il y a plusieurs Unités de saisie sur le site, il faut réaliser l'enrôlement sur chaque Unité de saisie.

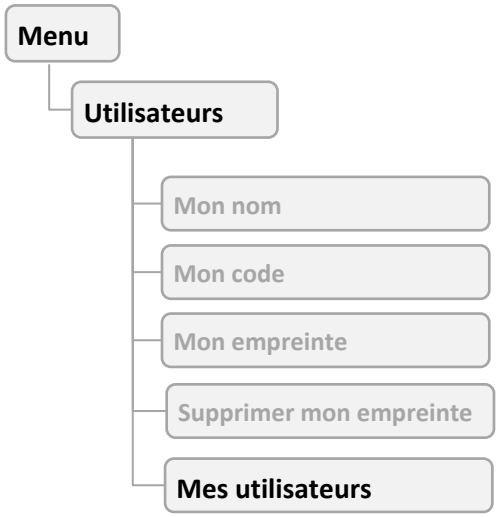
7.6 Suppression de l'empreinte à l'initiative de l'utilisateur

Etape	Ecran	Description
1		Sélectionnez la serrure + ENTER **Note** : pour ouvrir l'US 2, utilisez la flèche ▼ pour la sélectionner.
2		Utilisez la flèche ▼ pour sélectionner **Accès au menu** + ENTER
3		Tapez votre identifiant + ENTER Tapez votre code PIN + ENTER Suivez les instructions pour le contrôle de l'empreinte.
4		Appuyez sur ENTER Pour un utilisateur sans reconnaissance d'empreinte, passez à l'étape **5** ; sinon, passez à l'étape **6**.
5		Utilisez la flèche ▼ pour sélectionner **Supprimer mon empreinte** + ENTER.
6		Confirmez la suppression avec OUI ou NON pour annuler la procédure

En mode **Code + empreinte digitale**, si l'utilisateur quitte la procédure d'enrôlement, la procédure d'enregistrement est lancée automatiquement la première fois que l'utilisateur effectue une procédure d'ouverture.

S'il y a plusieurs Unités de saisie sur le site, il faut réaliser la suppression de l'empreinte sur chaque Unité de saisie.

Si l'utilisateur n'a pas le droit de changer son code, le Manager (ou super Manager) peut effacer l'empreinte de l'utilisateur :



- Appuyez sur ENTER.
- Sélectionnez **Suppression de l'empreinte** avec ENTER.
- Confirmez la suppression ou non avec OUI et NON.
  - Si oui, l'effacement commence.
  - Sinon, retour à l'écran précédent.

Les différents paramètres sont accessibles en fonction des droits de l'utilisateur concerné.

7.7 Suppression de toutes les empreintes

Voir chapitre 4.2.

8 SECURISATION

Par défaut, la communication avec les périphériques se fait de manière cryptée en utilisant une **clé d'authentification d'usine**.
Pour améliorer la sécurisation, il est préférable de modifier les clés d'authentification.

La sécurisation d'une installation **KeINet@** est obligatoire dans les cas suivants :

- Installation de type « **distributed system** ». C'est le cas lorsque le bus de communication entre l'Unité de saisie et l'Unité de Sécurité passe à l'extérieur du coffre.
- Installation « **IP** ».

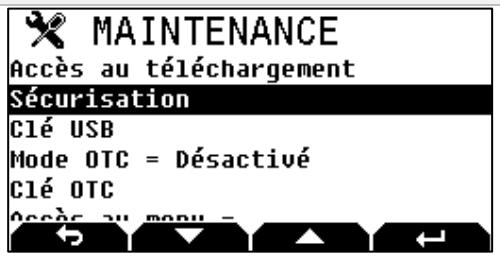
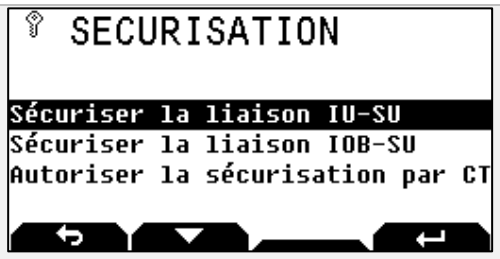
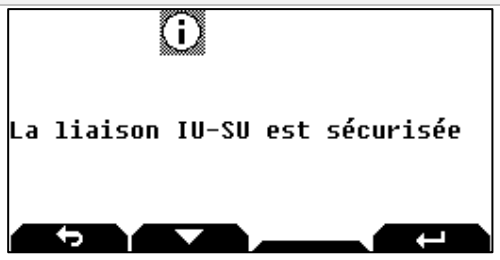
8.1 Sécurisation par l'Unité de saisie

Cette sécurisation est faite directement par l'Unité de saisie.

Elle ne peut être mise en œuvre que pour de très petites installations : 1 ou 2 serrures.

Pour de plus grosses configurations, il faut réaliser la sécurisation à partir de l'**Outil de Configuration (CT)**.

La procédure de sécurisation par l'Unité de saisie est la suivante :

Etape	Ecran	Description
1		Entrez dans le menu de l'Unité de saisie avec le code Super Manager. Sélectionnez **Maintenance** + ENTER
2		Sélectionnez **Sécurisation** + ENTER
3		Sélectionnez **Sécuriser la liaison IU-SU** + ENTER
4		La liaison IU – SU est maintenant sécurisée. Répétez cette opération avec toutes les SU.

8.2 Sécurisation avec l'Outil de Configuration

Cette sécurisation est faite directement en utilisant l'Outil de Configuration (CT).

Elle nécessite d'utiliser un ticket KelNet délivré uniquement par le Service Support de **Fichet Technologies**.

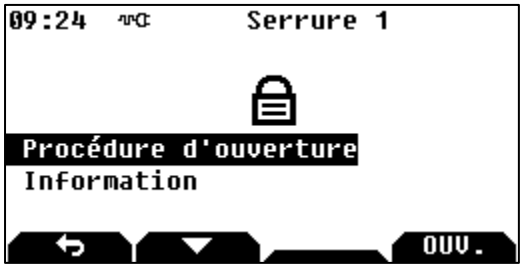
Elle permet de sécuriser en une seule fois tous les périphériques du site.

La sécurisation par le CT peut être réalisée même si des liaisons ont déjà été sécurisées directement sur l'Unité de saisie.

9 SPECIFICITES POUR UNE SERRURE REDONDANTE

La serrure redondante fonctionne de la même façon que la serrure standard.

En cas de dysfonctionnement d'une partie de la serrure, l'accès au menu n'est plus possible et donc lors de la sélection de la serrure, l'écran suivant s'affiche :



Lors de la sélection de la procédure d'ouverture, le message d'erreur suivant apparaît :

Les procédures d'ouverture et de fermeture de la serrure sont toujours possibles, suivant les paramètres programmés.

10 PARAMETRES USINE

Les paramètres usine par défaut sont :

	Identification / code PIN		Droits	Droit d'ouverture	Planning
Super Manager 1	1 – 00000000	**Actif**	Tous	Non	6
Manager 1	2 – 00000000	**Actif**	Changer codes 3 à 19	Oui	1
Opérateur 01 à Opérateur 17	3 - 00000000 à 19 – 00000000	Inactif	Non	Oui	1
Manager 2	20 – 00000000	Inactif	Changer codes 21 à 29	Oui	2
Opérateur 1 Bio à Opérateur 9 Bio	21 - 00000000 à 29 – 00000000	Inactif	Non	Oui	2
Manager CIT	30 – 00000000	Inactif	Changer codes 31 à 39	Oui	3
Opérateur CIT 1 à Opérateur CIT 9	31 - 00000000 à 39 – 00000000	Inactif	Non	Oui	3
Super Manager 2	99 - 00000000	Inactif	Tous	Non	6

Plannings :

- Planning 1 : 6h à 22h tous les jours.
- Planning 2 : 6h à 22h tous les jours.
- Planning 3 : 0h à 24h tous les jours.
- Planning 6 : 0h à 24h tous les jours.

Aucun planning annuel, aucune fermeture exceptionnelle, aucune ouverture exceptionnelle et aucun jour férié n'est défini.

Retards :

- Retard à l'ouverture = 1 minute.
- Retard d'alarme sous contrainte = 10 minutes.
- Retard de blocage d'urgence = 30 minutes.
- Retard de blocage automatique après une procédure d'ouverture = 0.
- Timeout de pêne rentré = 10 minutes.

Paramètres généraux :

- Mode alarme sous contrainte = dernier digit + 1.
- Règle de blocage faux code = "Blocage croissant".
- Pas d'asservissements.
- Pas de mode « 4 yeux ».
- Pas de procédure de fermeture par identification.
- Pas de ré-identification après retard.
- Pas de fonction sur les entrées/sorties.

11 RECYCLAGE

L'Unité de Sécurité et l'Unité de saisie peuvent être recyclées.

Il y a différents niveaux de recyclage :

1. Recyclage des clés d'authentification (utilisées pour la sécurisation).
2. Recyclage de l'adresse du périphérique.
3. Recyclage complet des paramètres de fonctionnement.

L'audit de la serrure n'est jamais effacé.

11.1 Recyclage des clés d'authentification de l'Unité de Sécurité

Cette procédure permet de revenir aux clés d'authentification usine.

Pour effectuer un recyclage des clés d'authentification de l'Unité de Sécurité, il faut faire les opérations suivantes :

1. Coupez l'alimentation de l'Unité de Sécurité. Si le câble USB est connecté à l'Unité de saisie, il faut le débrancher.
2. Appuyez sur le bouton de l'Unité de Sécurité : cela permet de réveiller le microprocesseur de l'Unité de Sécurité et donc de décharger les condensateurs de l'alimentation, sinon le microprocesseur va rester actif et il n'y aura pas de redémarrage.
3. Rebranchez l'alimentation : la led verte de l'Unité de Sécurité va clignoter (10 secondes au maximum).
4. Pendant le clignotement, appuyez **2 fois** sur le bouton poussoir de l'Unité de Sécurité : la led va clignoter plus rapidement.
5. Attendez la fin du clignotement.

11.2 Recyclage de l'adresse de l'Unité de Sécurité

Cette procédure permet :

- de revenir aux clés d'authentification usine.
- d'effacer l'adresse de l'Unité de Sécurité (valeur 127).

Il faut faire les opérations suivantes :

1. Coupez l'alimentation de l'Unité de Sécurité. Si le câble USB est connecté à l'Unité de saisie, il faut le débrancher.
2. Appuyez sur le bouton de l'Unité de Sécurité : cela permet de réveiller le microprocesseur de l'Unité de Sécurité et donc de décharger les condensateurs de l'alimentation, sinon le microprocesseur va rester actif et il n'y aura pas de redémarrage.
3. Rebranchez l'alimentation : la led verte de l'Unité de Sécurité va clignoter (10 secondes au maximum).
4. Pendant le clignotement, appuyez **5 fois** sur le bouton poussoir de l'Unité de Sécurité : la led devient fixe.
5. Attendez l'extinction de la led.

11.3 Recyclage complet de l'Unité de Sécurité

Pour effectuer un recyclage complet de l'Unité de Sécurité, il faut faire les opérations suivantes :

1. Coupez l'alimentation de l'Unité de Sécurité. Si le câble USB est connecté à l'Unité de saisie, il faut le débrancher
2. Appuyez sur le bouton de l'Unité de Sécurité : cela permet de réveiller le microprocesseur de l'Unité de Sécurité et donc de décharger les condensateurs de l'alimentation, sinon le microprocesseur va rester actif et il n'y aura pas de redémarrage.
3. Rebranchez l'alimentation : la led verte de l'Unité de Sécurité va clignoter (10 secondes au maximum).
4. Pendant le clignotement, appuyez **10 fois** sur le bouton poussoir de l'Unité de Sécurité : la led va clignoter plus rapidement puis elle devient fixe.
5. Attendez l'extinction de la led.

Après recyclage, tous les paramètres sont initialisés à la valeur « usine » (valeur par défaut) : voir Chapitre 10.

11.4 Recyclage des clés d'authentification de l'Unité de saisie

Cette procédure permet de revenir aux clés d'authentification usine.

Pour effectuer un recyclage des clés d'authentification de l'Unité de saisie, il faut faire les opérations suivantes :

1. Coupez l'alimentation de l'Unité de saisie. Si le câble USB est connecté à l'Unité de saisie, il faut le débrancher.
2. Démontez l'Unité de saisie.
3. Attendez 5 secondes.
4. Rebranchez l'alimentation : la led rouge de l'Unité de saisie va clignoter (10 secondes au maximum).
5. Pendant le clignotement, appuyez **2 fois** sur le switch anti-arrachement : la led rouge devient fixe.
6. Attendez l'extinction de la led.
7. Remontez l'Unité de saisie.

11.5 Recyclage complet de l'Unité de saisie

Pour effectuer un recyclage complet de l'Unité de saisie, il faut faire les opérations suivantes :

1. Coupez l'alimentation de l'Unité de saisie. Si le câble USB est connecté à l'Unité de saisie, il faut le débrancher.
2. Démontez l'Unité de saisie.
3. Attendez 5 secondes.
4. Rebranchez l'alimentation : la led rouge de l'Unité de saisie va clignoter (10 secondes au maximum).
5. Pendant le clignotement, appuyez **10 fois** sur le switch anti-arrachement : la led rouge devient fixe.
6. Attendez l'extinction de la led rouge.
7. Remontez l'Unité de saisie.

Tant que le switch anti-arrachement est ouvert, le message « **Anti-arrachement ouvert** » est affiché et seul l'accès au menu de l'Unité de saisie est autorisé.

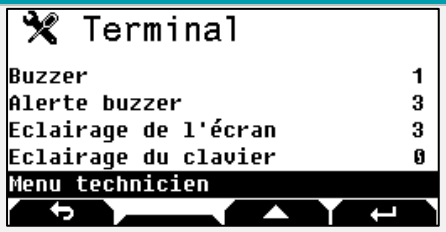
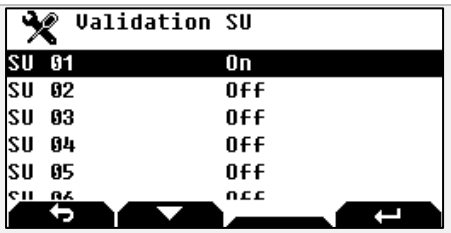
Sinon, le message suivant apparait :

Ce message est affiché tant qu'il n'y a pas eu une identification valide, mais il ne bloque pas la serrure.

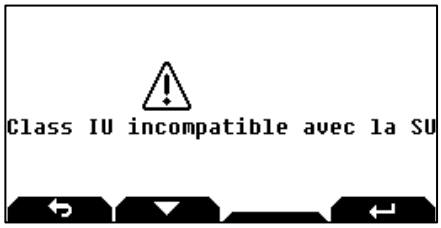
12 MAINTENANCE

12.1 Remplacement d'une Unité de saisie fonctionnant en mode usine

Après avoir branché la nouvelle Unité de saisie, il faut effectuer les opérations suivantes :

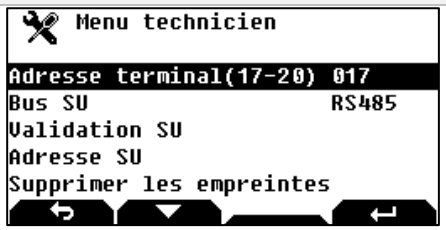
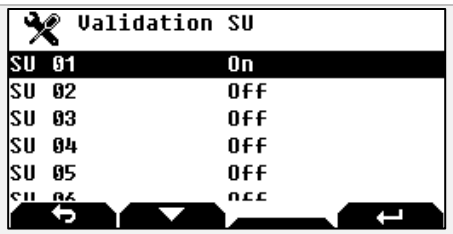
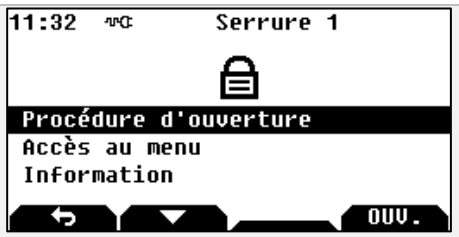
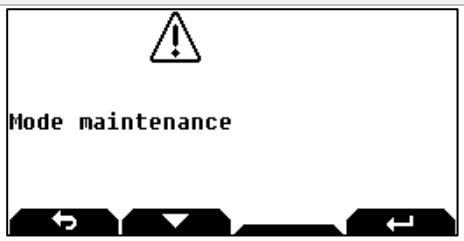
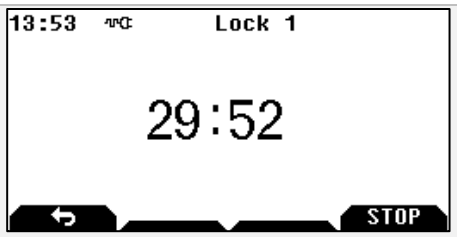
Etape	Ecran	Description
1		Sélectionnez le **Menu technicien** + ENTER **Nota :** Le **Menu Technicien** n'est visible que si le switch anti-arrachement de l'Unité de saisie est ouvert.
2		Configurez l'adresse de l'Unité de saisie (17 pour la 1ère Unité de saisie) et le type de bus : RS485 ou MF2
3		Sélectionnez le menu **Validation SU** et mettez à **ON** les serrures présentes
4		Revenez dans l'écran d'accueil. L'ensemble est à nouveau opérationnel.

Si la classe de l'Unité de saisie est A ou B et que la classe de l'Unité de Sécurité est C ou D, on ne pourra ni ouvrir la serrure ni entrer dans le menu de configuration de l'Unité de Sécurité. Le message suivant est affiché :



12.2 Remplacement d'une Unité de saisie sécurisée

Après avoir branché la nouvelle Unité de saisie, il faut effectuer les opérations suivantes :

Etape	Ecran	Description
1		Sélectionnez le **Menu technicien** + ENTER **Nota :** Le **Menu Technicien** n'est visible que si le switch anti-arrachement de l'Unité de saisie est ouvert.
2		Configurez l'adresse de l'Unité de saisie (17 pour le 1ère Unité de saisie) et le type de bus : RS485 ou MF2.
3		Sélectionnez le menu **Validation SU** et mettez à **ON** les serrures présentes.
4		Revenez dans l'écran d'accueil.
5		Sélectionnez la serrure, puis après la phase authentification, faites une commande d'ouverture. **Nota :** A ce stade, l'accès au menu est interdit et le message **Mode maintenance** est affiché.
6		Si l'on fait une procédure d'ouverture, le message suivant apparait pour indiquer que la serrure est en mode « maintenance » car l'Unité de saisie ne possède pas la même clé d'authentification que l'Unité de Sécurité mais uniquement la clé usine.
7		Après avoir saisi le code d'ouverture, il faudra attendre un délai plus long que le délai normal d'ouverture. Ce délai est défini par le paramètre **Retard changement terminal** qui est de 30 minutes par défaut.

Lorsque la porte est ouverte, on pourra accéder à l'Unité de Sécurité.

Il faut ensuite réinitialiser la clé d'authentification de l'Unité de Sécurité (voir chapitre 11.1).

A ce stade, l'Unité de saisie et l'Unité de Sécurité fonctionnent avec la clé d'authentification usine.

Il faut donc refaire la phase de sécurisation de l'ensemble IU-SU.

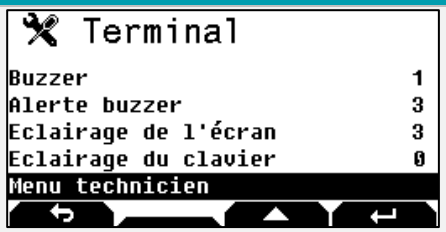
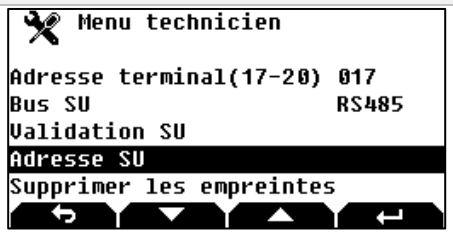
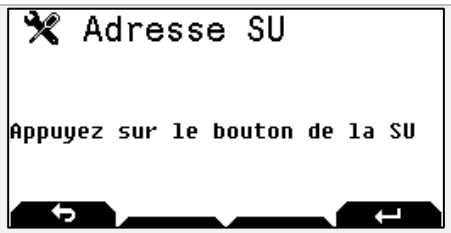
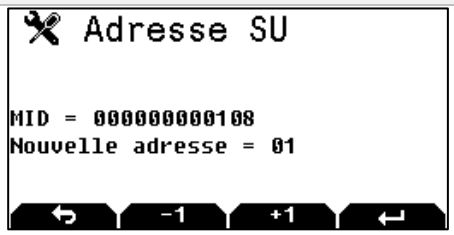
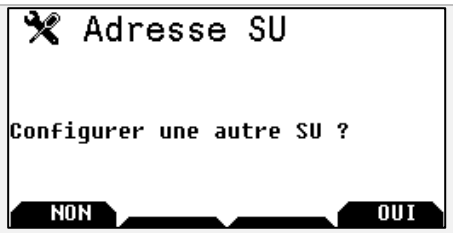
Si la classe de l'Unité de saisie est A ou B et que la classe de l'Unité de Sécurité est C ou D, on ne pourra ni ouvrir la serrure ni entrer dans le menu de configuration de l'Unité de Sécurité. Le message suivant est affiché :

12.3 Remplacement d'une SU fonctionnant en mode usine

En cas de panne d'une Unité de Sécurité, il faut d'abord pouvoir accéder à celle-ci.

La nouvelle Unité de Sécurité doit être configurée « départ usine ». Si ce n'est pas le cas, il faut procéder à un recyclage de l'Unité de Sécurité.

Après avoir branché la nouvelle Unité de Sécurité, il faut effectuer les opérations suivantes :

Etape	Ecran	Description
1		Sélectionnez le **Menu technicien** + ENTER **Nota :** Le **Menu Technicien** n'est visible que si le switch anti-arrachement de l'Unité de saisie est ouvert.
2		Sélectionnez le menu **Adresse SU**.
3		Appuyez sur le bouton poussoir de la SU.
4		Saisissez la même adresse que la serrure qui a été démontée (de 1 à 16), puis validez
5		Comme il n'y a pas d'autre SU à changer, appuyez sur **NON**.

Il faut ensuite reconfigurer l'Unité de Sécurité et saisir tous les codes usagers.

12.4 Remplacement d'une SU sécurisée

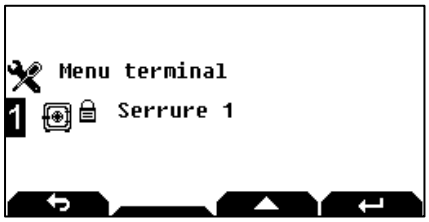
Il faut d'abord procéder comme pour une SU fonctionnant en mode usine (voir chapitre 12.3).

A ce stade, si l'on veut faire une procédure d'ouverture ou un accès au menu, on aura le message suivant :

Ce message est affiché parce que l'Unité de saisie est sécurisée, mais pas l'Unité de Sécurité.

Il faut donc effacer les clés authentification de l'Unité de saisie (voir chapitre 11.4).

Sélectionnez la serrure et validez :



L'authentification est réalisée avec succès, mais la liaison IU-SU n'est pas sécurisée.

Il faut donc procéder à la sécurisation de la liaison IU-SU (voir chapitre 8.1).

Si plusieurs Unités de Sécurité sont branchées sur l'Unité de saisie, il faut recycler toutes les Unités de Sécurité et refaire la sécurisation de toutes les liaisons IU-SU.

13 GLOSSAIRE

Bouton SU
Ce bouton est utilisé pour fixer l'adresse de l'Unité de Sécurité et pour effectuer les opérations de recyclage.

Carte E/S
Carte d'interface utilisée pour augmenter le nombre d'entrées et de sorties sur la serrure.

Centre national de prévention et de protection (CNPP)
Centre national de prévention et de protection chargé de l'homologation des produits.

CIT - Cash In Transfer
Transporteur de fonds, pour la livraison et le ramassage des fonds.

Code
Information d'identification qui peut être rentrée sur une Unité de saisie et qui permet l'autorisation de changer le statut ou les paramètres de la serrure.

Code d'alarme sous contrainte
Code parallèle initiant des fonctions supplémentaires (modification du retard, alarme).

Code Biométrique
Code prenant en compte les caractéristiques du corps humain (empreinte biométrique).

CT (Configuration Tool) = Outil de Configuration
Logiciel sur le PC qui est utilisé pour configurer tous les paramètres d'une HSL.

DOCT – Détection Ouverture Choc et Thermique
Signal d'alarme de détection de choc et de température.

Entrée contact sec
Entrée sans tension (switch, contact de relais).

Evènements
Journal chronologique des évènements de la serrure (aussi : "journal des évènements").

Filtre angulaire
Filtre optique angulaire placé sur l'écran pour limiter la vision angulaire (nécessaire pour la classe C).

G1 – Procédure G1
Quand une "procédure G1" est paramétrée pour une SU, les identifications ne sont pas autorisées. L'activation de cette procédure autorise l'accès pendant un temps ajustable (15 à 180'').

G2 – Procédure G2
Quand une "procédure G2" est paramétrée pour une SU et activée, le retard à l'ouverture est annulé.

G3 – Procédure G3
Quand une "procédure G3" est paramétrée pour une SU et activée, la procédure en cours est annulée.

G4 – Procédure G4
Quand une "procédure G4" est paramétrée pour une SU et activée, le retard à l'ouverture est remplacé par un retard « de substitution ».

Homologation
Niveau de certification du produit. Sous certaines conditions, l'homologation peut être perdue (identification par empreinte biométrique seulement par exemple).

HSL - High Security Lock
Serrure de Haute Sécurité associée au montage de portes ou coffre de sécurité, sur laquelle des codes peuvent être saisie et comparés aux codes mémorisés (dans l'unité de sécurité). Une comparaison correcte d'un code ouvrant autorise le mouvement du pêne d'une unité de blocage.

ID - Identifiant
Méthode d'identification d'un utilisateur. Pour KeINet, l'identifiant est un nombre de 1 à 99 pour un usager connu de l'Unité de Sécurité. Dans le cas d'un code OTC, l'identifiant est défini sur 4 digits ou plus.

IO-Box (Input Output Box) = carte entrées / sorties
Périphérique permettant de gérer plus d'entrées / sorties.

IP-Box
Périphérique d'interface utilisé pour convertir une liaison série RS485 vers une liaison Ethernet.

Journal des évènements
Journal chronologique des évènements (voir aussi : audit).

MF2
Nom du bus/protocole utilisé entre les Unités de saisie et les Unités de Sécurité de la serrure KeINet.

Mode 4 yeux
Ce mode nécessite l'identification de deux utilisateurs différents pour valider une procédure d'ouverture ou d'accès aux menus.

OTC - One Time Code
Code limité dans le temps et en nombre d'utilisation.

Pêne (ou élément bloqueur)
Partie d'une HSL qui, après une identification correcte, peut bouger, ou peut-être bougée, pour sécuriser une porte ou empêcher le mouvement de la tringlerie.

PIN - Personal Identification Number
Mot de passe ou code secret connu de l'utilisateur seulement et permettant de l'identifier.

Recyclage
Procédure de réinitialisation des paramètres d'un périphérique.

Règles d'asservissement
Règles définissant les conditions validant la procédure d'ouverture.

RS485
Nom du bus utilisé entre les différents périphériques de la serrure KeINet, compatible avec la norme EIA-485.

Statut de la porte
Les statuts normalisés de la porte d'une HSL sont :

- **Porte fermée :** la porte est fermée et les pênes prêts à être engagés dans leur gâche.
- **Porte verrouillée :** les pênes sont engagés dans leur gâche.
- **Porte bloquée :** la tringlerie ne peut pas être déverrouillée à cause de la HSL.
- **Porte sécurisée :** la porte est fermée, bloquée et condamnée par une HSL à l'état sécurisé (ne peut être déverrouillée que par un code d'ouverture).

SU (Secure Unit) = Unité de Sécurité
Partie d'une HSL qui analyse les code saisis et autorise ou empêche le mouvement du pêne.

Tringlerie
Système de tringlerie de la porte. Un switch de tringlerie indique si la porte peut être ouverte ou non.

Unité de saisie - Terminal
Partie d'une HSL qui communique les codes à l'Unité de Sécurité.

USB –Universal Serial Bus
Bus série standard pour interfacer un périphérique avec un PC hôte.

Verrou (ou unité de blocage)
Pêne mobile qui autorise ou empêche le mouvement d'un élément de blocage.