Kaspersky Mobile Security 9
for Symbian

Guide de l'utilisateur

VERSION DE L'APPLICATION : 9.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que cette documentation vous sera utile dans votre travail et vous apportera toutes les réponses sur notre produit logiciel.

Ce document peut être modifié sans préavis. Pour obtenir la dernière version de ce document, reportez-vous au site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.

Date d'édition : 24/10/2011

http://www.kaspersky.com/fr
http://support.kaspersky.fr/

TABLE DES MATIERES

A PROPOS DE CE MANUEL

Ce document est le guide de l'utilisateur de Kaspersky Mobile Security.

Afin de profiter au maximum des possibilités de Kaspersky Mobile Security, les utilisateurs doivent maîtriser leur appareil nomade : connaissance de l'interface du système d'exploitation utilisé, connaissances fondamentales des principales opérations et maniement du courrier électronique et d'Internet.

Ce guide poursuit les objectifs suivants :

- aider à installer, activer et utiliser Kaspersky Mobile Security ;
- offrir un accès rapide aux informations pour répondre aux questions liées à Kaspersky Mobile Security ;
- présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

Sources d'informations complémentaires

Cette section contient des informations supplémentaires concernant l'application et les ressources Internet où vous pouvez discuter de l'application, échanger des idées, poser des questions et obtenir des réponses.

Kaspersky Mobile Security 9

Cette section contient une description des fonctionnalités de l'application et offre des informations succinctes sur ses composants et leurs fonctions principales. Cette section contient les informations concernant le pack livré. La section décrit également la configuration matérielle et logicielle requises pour l'installation de Kaspersky Mobile Security 9.

Installation de Kaspersky Mobile Security 9

Cette section contient les instructions qui vous aideront à installer l'application sur l'appareil mobile.

Suppression de l'application

Cette section contient les instructions qui vous aideront à supprimer l'application de l'appareil mobile.

Mise à jour de l'application

Cette section contient les instructions qui vous aideront à mettre à jour la version de l'application.

Premiers pas

Cette section contient les informations sur le début de l'utilisation de Kaspersky Mobile Security 9 : activation de l'application, saisie du code secret, activation de la fonction de restauration du code secret, lancement du programme, mise à jour des bases antivirus et lancement de l'analyse antivirus de l'appareil.

Gestion de la licence

Cette section contient les informations sur les concepts de base utilisées pour l'octroi de licence de l'application. La section présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Mobile Security 9 et de la renouveler.

Interface de l'application

Cette section présente des informations sur les principaux composants de l'interface de Kaspersky Mobile Security 9.

Protection du système de fichiers

La section présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. La section explique aussi comment activer / suspendre la protection et la configurer.

Analyse de l'appareil

Cette section présente les informations sur l'analyse de l'appareil à la demande, qui permet d'identifier et de neutraliser les menaces sur votre appareil. De plus, la section décrit comment lancer l'analyse de l'appareil, comment configurer l'analyse programmée du système de fichiers, comment sélectionner les fichiers à analyser et définir l'action de l'application en cas de détection d'un objet malveillant.

Quarantaine des objets malveillants

La section présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. De plus, elle décrit comment consulter, restaurer ou supprimer les objets malveillants stockés dans le dossier.

Filtrage des appels et des SMS entrants

Cette section présente les informations sur le Filtre des appels et SMS qui interdit la réception d'appels et des SMS non sollicités sur la base des listes noire et blanche que vous avez créées. De plus, la section indique comment sélectionner le mode Filtre des appels et SMS pour les appels et les SMS entrants, comment configurer les paramètres avancés de filtrage pour les appels et les SMS entrants et comment créer la liste noire et la liste blanche.

Restrictions sur les appels et les SMS sortants. Contrôle Parental

Cette section présente le composant Contrôle parental qui permet de restreindre les appels et les SMS sortants à certains numéros. Elle explique également comment composer des listes de numéros interdits ou autorisés et configurer les paramètres du Contrôle parental.

Protection des données en cas de perte ou de vol de l'appareil

La section présente le composant Antivol, qui protège les données stockées sur l'appareil mobile contre l'accès non autorisé en cas de perte ou de vol, toute en facilitant sa recherche.

Elle explique également comment activer/désactiver les fonctions d'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la fonction Antivol depuis un autre appareil mobile.

Dissimulation des informations personnelles

La section présente le composant Contacts personnels, qui permet de dissimuler les données confidentielles de l'utilisateur.

Filtrage de l'activité de réseau. Pare-feu

La section présente le composant Pare-feu, qui contrôle les connexions de réseau sur votre appareil. De plus, elle décrit comment activer / désactiver le composant Pare-feu et comment sélectionner le mode de fonctionnement requis.

Chiffrement des données personnelles

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. De plus, la section décrit comment chiffrer et déchiffrer les dossiers sélectionnées.

Mise à jour des bases du programme

La section présente la mise à jour des bases anti-virus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

Journaux du logiciel

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus).

Configuration des paramètres complémentaires

La section présente les informations sur les fonctionnalités complémentaires de Kaspersky Mobile Security 9 : comment modifier le code secret, comment administrer les notifications sonores de l'application et le rétro-éclairage, et comment activer / désactiver l'affichage des astuces, de l'icône de protection ou de la fenêtre d'état de la protection.

Contacter le Service d'assistance technique

Cette section contient des recommandations pour contacter Kaspersky Lab en utilisant l'espace personnel du Service d'assistance technique du site ou par téléphone.

Glossaire

Cette section contient la liste des termes présents dans le document ainsi que leurs définitions.

Kaspersky Lab

La section reprend les informations relatives à Kaspersky Lab.

Informations sur le code tiers

La section reprend les informations relatives au code tiers utilisé dans l'application.

Index

Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
Veuillez noter que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations ou à la perturbation du fonctionnement de l'appareil mobile.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<adresse IP de votre appareil mobile>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du support technique (base de connaissances) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la réponse à votre question, vous pouvez contacter le service d'assistance technique de Kaspersky Lab" (cf. section "Assistance technique par téléphone" à la page 125).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Web de Kaspersky Lab.

Page sur le site Web de Kaspersky Lab

Le site Web de Kaspersky Lab contient une page particulière pour chaque application.

La page (http://www.kaspersky.com/fr/kaspersky_mobile_security) fournit des informations générales sur l'application, ces possibilités et ses particularités.

La page http://www.kaspersky.com/fr/ contient le lien sur la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page de l'application sur le serveur du Support technique (Knowledge Base)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Mobile Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide contextuelle.

L'aide contextuelle contient des informations sur chacun des onglets et fenêtres de Kaspersky Mobile Security : liste et description des paramètres.

Documentation

Le guide de l'utilisateur contient les informations sur l'installation, sur l'activation, sur la configuration des paramètres, ainsi que les informations pour travailler avec l'application. Le document décrit l'interface graphique et décrit l'exécution des tâches les plus fréquentes dans l'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.com/).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONTACTER LE DÉPARTEMENT COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service commercial à l'aide d'un des moyens suivants :

- En appelant notre service clientèle Français (détails sur http://www.kaspersky.com/fr/contacts).
- En envoyant un message avec votre question par .

Le service est offert en russe et en anglais.

CONTACTER LE GROUPE DE RÉDACTION DE LA DOCUMENTATION PAR COURRIER ÉLECTRONIQUE

Pour contacter le Groupe de rédaction de la documentation, vous pouvez envoyer un message par courrier électronique. En tant que sujet du message, il faut indiquer "Kaspersky Help Feedback: Kaspersky Mobile Security".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 protège les appareils nomades (ci-après les "appareils") tournant sous Symbian OS. L'application protège les données de l'appareil contre l'infection par des menaces connues, refuse les SMS et les appels non sollicités, contrôle les connexions de réseau de l'appareil, chiffre les données, masque les informations pour les contacts confidentiels et protège les données confidentielles en cas de perte ou de vol de l'appareil. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier.

Kaspersky Mobile Security 9 reprend les composants suivants pour la protection :

- **Anti-Virus**. Protège le système de fichiers de l'appareil mobile contre les virus et autres programmes malveillants. Antivirus permet d'identifier et de neutraliser les objets malveillants sur votre appareil, ainsi que de mettre à jour les bases antivirus de l'application.

- **Filtre app./SMS**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant permet de configurer en souplesse la fonction de blocage des SMS et des appels considérés comme indésirables.

- **Antivol**. Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol tout en facilitant sa recherche. Antivol permet de verrouiller l'appareil à distance à l'aide des SMS, de supprimer les données qu'il contient et de déterminer ses coordonnées géographiques (si l'appareil mobile est doté d'un récepteur GPS). De plus, Antivol permet également de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.

- **Ctrl parental**. Contrôle tous les SMS et les appels sortants. Le composant permet de configurer en souplesse le filtrage des SMS et des appels sortants.

- **Contacts personnels**. Masque les informations liées aux numéros confidentiels de la Liste des contacts que vous avez créée. Les Contacts personnels masquent les entrées des Contacts, les SMS, les entrées dans le journal des appels, les SMS reçus et les appels entrants pour ce type de numéros.

- **Pare-feu**. Contrôle les connexions de réseau de votre appareil mobile. Le Pare-feu permet de définir les connexions qui seront autorisées ou interdites.

- **Chiffrement**. Stocke les données en mode crypté. Le composant Chiffrement permet de crypter un nombre quelconque de dossiers qui ne sont pas définis par le système et enregistrés aussi bien dans la mémoire de l'appareil que sur les cartes mémoire. L'accès aux fichiers depuis les dossiers chiffrés est offert uniquement après avoir saisi le code secret de l'application.

Outre cela, l'application propose diverses fonctions de service permettant de maintenir l'application dans un état actuel, élargir les possibilités d'utilisation de l'application, et ceux qui aide l'utilisateur à travailler :

- Etat de la protection. Les états des composants de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection des données stockées sur l'appareil.

- La mise à jour des bases antivirus de l'application. La fonction permet de tenir à jour les bases antivirus de Kaspersky Mobile Security 9.

- Journal des événements. Les informations sur le fonctionnement de chacun des composants (par exemple, rapport d'analyse, mise à jour des bases antivirus, détails sur un fichier bloqué) sont consignées dans un journal des événements spécifique. Les rapports sur le fonctionnement des composants sont envoyés et stockés dans le système d'administration distante.

Kaspersky Mobile Security 9 n'effectue pas la copie de sauvegarde de l'information et la restauration ultérieure.

DANS CETTE SECTION

NOUVEAUTES DE KASPERSKY MOBILE SECURITY 9

Voici une présentation détaillées des nouveautés de Kaspersky Mobile Security 9.

Les nouvelles possibilités suivantes sont réalisées dans Kaspersky Mobile Security 9 :

- L'accès au programme est régi par un mot de passe.
- Pour les contacts confidentiels de la liste des contacts, le composant Contacts personnels permet de masquer les informations suivantes : entrées dans les Contacts, SMS, journal des appels, SMS reçus et appels entrants. Les informations confidentielles sont accessibles si la fonction de dissimulation est désactivée.
- Le composant Chiffrement permet de chiffrer les dossiers enregistrés dans la mémoire de l'appareil ou sur une carte mémoire. Le composant stocke les informations confidentielles en mode crypté et ne permet d'accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application.
- L'application propose également une nouvelle fonction de service Affichage des astuces : Kaspersky Mobile Security 9 affiche une brève description du composant avant la configuration de ses paramètres.
- Vous pouvez directement acheter le code d'activation et renouveler la durée de validité de la licence depuis l'appareil mobile à l'aide de la fonction d'abonnement ou en ligne.

KIT DE DISTRIBUTION

Vous pouvez acquérir Kaspersky Mobile Security 9 par Internet (le kit de distribution et la documentation du programme sont au format numérique). Vous pouvez également acquérir Kaspersky Mobile Security 9 revendeurs de téléphonie mobile. Pour des détails sur la méthode d'achat et le kit de distribution, contactez notre Département commercial au info@kaspersky.fr.

SERVICE POUR LES UTILISATEURS ENREGISTRES

L'achat d'une licence vous donne le statut d'utilisateur enregistré tout au long de la durée de sa validité, ce qui vous permet de bénéficier des services suivants :

- Mise à jour des bases et nouvelles versions de l'application ;
- Support par téléphone et par courrier électronique sur toutes les questions en rapport avec l'installation, la configuration et l'utilisation de l'application ;
- Notification sur les nouvelles applications de Kaspersky Lab et les nouveaux virus référencés. Afin bénéficier de ce service, vous devrez vous abonner à la liste de diffusion des informations de Kaspersky Lab ZAO présente sur le site Internet du service d'assistance technique.

Aucun support ne sera apporté sur l'utilisation du système d'exploitation ou des logiciels tiers.

SPECIFICATIONS MATERIELLES ET LOGICIELLES

Kaspersky Mobile Security 9 peut être installé sur des appareils mobiles avec des systèmes d'exploitation Symbian OS 9.1, 9.2, 9.3 et 9.4 Series 60 UI.

INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section fournit des informations sur l'installation et la suppression de l'application.

INSTALLATION DE KASPERSKY MOBILE SECURITY 9

L'installation de l'application sur l'appareil nomade s'effectue en plusieurs étapes.

Pour installer Kaspersky Mobile Security 9, procédez de la manière suivante :

1. Connectez l'appareil nomade à l'ordinateur.

   Pour les appareils nomades de la marque Nokia, il est conseillé d'utiliser l'application Nokia PC Suite ou Nokia Ovi Suite.

2. Exécutez une des opérations suivantes :

   - Si vous avez acheté l'application sur un cédérom, lancez l'installation automatique de Kaspersky Mobile Security 9 depuis ce cédérom.

   - Si vous avez obtenu le fichier d'installation via Internet, copiez-le sur l'appareil nomade. Pour ce faire, appliquez l'une des méthodes suivantes :

     - utilisez l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;

     - utilisez une carte d'extension mémoire.

     Puis lancez l'installation avec l'une des méthodes suivantes :

     - depuis l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;

     - en ouvrant l'archive SIS de la distribution sur l'appareil nomade.

   L'écran de confirmation de l'installation s'ouvre.

3. Pour confirmer l'installation de l'application, cliquez sur **Oui**.

4. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.

   Si la langue du système d'exploitation ne correspond pas à la langue de Kaspersky Mobile Security 9, un message s'affiche. Pour continuer l'installation de l'application dans la langue actuelle, cliquez sur **OK**.

5. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. L'installation de Kaspersky Mobile Security 9 est lancée. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.

6. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade en cliquant sur **OK**.

7. Pour terminer l'installation, redémarrez l'appareil.

   L'application sera installée avec les paramètres recommandés par les experts de Kaspersky Lab.

MISE A JOUR DE L'APPLICATION

Vous pouvez mettre à jour Kaspersky Mobile Security 9 en installant la version la plus récente de cette génération (par exemple, réaliser la mise à jour de la version 9.0 à la version 9.2).

Si vous utilisez Kaspersky Mobile Security 8.0, vous pouvez passer à la version Kaspersky Mobile Security 9.

Pour mettre l'application à jour, procédez comme suit :

1. Déchiffrez les données sur votre appareil si elles avaient été cryptées à l'aide de Kaspersky Mobile Security (cf. section "Déchiffrement des données" à la page 110).
2. Désactivez Contacts personnels (cf. section "Présentation des modes de Contacts personnels" à la page 95).
3. Quittez la version actuelle de Kaspersky Mobile Security 9. Pour ce faire, choisissez **Options** → **Quitter**.
4. Copiez le fichier d'installation de l'application sur l'appareil nomade. Pour ce faire, appliquez l'une des méthodes suivantes :
   - depuis le site Internet de "Kaspersky Lab" ;
   - utilisez l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;
   - utilisez une carte d'extension mémoire.
5. Exécutez le fichier d'installation de Kaspersky Mobile Security 9 sur l'appareil.
6. Pour confirmer l'installation de l'application, cliquez sur **Oui**.
7. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.
8. Confirmez la mise à jour de l'application en appuyant sur **OK**.
9. Saisissez le code secret défini dans la version antérieure de l'application.
10. Lisez attentivement le contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.
11. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade. Pour ce faire, cliquez sur **OK**.
12. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :
    - Si vous souhaitez conserver les paramètres de l'application et les objets en quarantaine, cochez la case en regard des paramètres requis, puis cliquez sur **OK**.
    - Pour supprimer complètement une application, cliquez sur **Annuler**.

    L'installation de Kaspersky Mobile Security 9 est lancée.
13. Pour terminer l'installation, redémarrez l'appareil.

    Si la durée de validité de la licence actuelle n'est pas écoulée, alors l'application sera activée automatiquement. Si la durée de validité de l'application est écoulée, activez l'application (cf. section "Activation de l'application" à la page 18).

Pour passer de Kaspersky Mobile Security 8.0 à la version 9, procédez comme suit :

1. Déchiffrez toutes les données si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security 8.0.

2. Fermez Kaspersky Mobile Security 8.0. Pour ce faire, choisissez **Options** → **Quitter**.
3. Désinstallation de Kaspersky Mobile Security 8.0. Pour ce faire, exécutez les actions suivantes :
   a. Ouvrez le menu principal de l'appareil.
   b. Sélectionnez le dossier **Applications** → **Install.**

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

   c. Dans la liste des applications, sélectionnez **KMS 8.0**, puis choisissez **Options** → **Supprimer**.
   d. Pour confirmer la suppression de l'application, cliquez sur **Oui**.
   e. Supprimez complètement les paramètres de Kaspersky Mobile Security 8.0 car ils sont incompatibles avec les paramètres de la version 9. Pour ce faire, cliquez sur **Annuler**.
4. Redémarrez l'appareil pour terminer la suppression de Kaspersky Mobile Security 8.0.
5. Passez à l'installation de Kaspersky Mobile Security 9 (cf. section "Installation de Kaspersky Mobile Security 9" à la page 16).

   Si la licence pour Kaspersky Mobile Security 8.0 est toujours valide, activez la version 9 à l'aide du code d'activation de la version 8.0 (cf. section "Activation de l'application" à la page 18).

ACTIVATION DU LOGICIEL

Avant de commencer le travail avec l'application Kaspersky Mobile Security 9, il faut l'activer.

Afin de pouvoir activer Kaspersky Mobile Security 9, la connexion à Internet doit être configurée sur l'appareil.

Avant d'activer l'application, assurez-vous que la date et l'heure système sont correctes.

Vous pouvez activer l'application d'une des manières suivantes :

- **Activer la version d'évaluation**. Lors de l'activation de la version d'évaluation de l'application, l'utilisateur reçoit une licence d'évaluation gratuite. La durée de validité de la licence d'évaluation est affichée à l'écran après l'activation. Une fois la durée de la licence d'évaluation écoulée, les possibilités de l'application sont réduites. Seules les fonctions suivantes sont accessibles :
  - activation du logiciel ;
  - administration de la licence de l'application ;
  - aide de Kaspersky Mobile Security 9 ;
  - désactivation de Chiffrement ;
  - désactivation de Contacts personnels.

  Il est impossible d'activer une deuxième fois la version d'évaluation.
- **Activer la version commerciale**. L'activation de la version commerciale s'opère à l'aide du code d'activation obtenu à l'achat de l'application. Dans le cadre de l'activation de la version commerciale, l'application obtient une licence commerciale qui permet d'utiliser toutes les fonctions de l'application. La durée de validité de la

licence apparaît à l'écran de l'appareil. Une fois la licence parvenue à échéance, les fonctionnalités de l'application sont restreintes et la mise à jour de l'application n'a plus lieu.

Vous pouvez obtenir le code d'activation d'une des manières suivantes :

- en ligne, en passant de l'application Kaspersky Mobile Security 9 au site Web de Kaspersky Lab dédiés aux appareils mobiles ;
- dans la boutique en ligne de Kaspersky Lab (http://kaspersky.telechargement.fr/);
- chez un revendeur de Kaspersky Lab.

- **Activer l'abonnement**. Lors de l'activation de l'abonnement, l'application reçoit une licence commerciale à abonnement. La durée de validité de la licence à abonnement est limitée à 30 jours. Dans le cadre de l'abonnement, l'application renouvelle la licence tous les 30 jours. Lors du renouvellement de la licence, la somme définie lors de l'activation de l'abonnement est débitée de votre compte personnel pour l'utilisation de l'application. Le paiement s'opère via l'envoi d'un SMS payant. Une fois que la somme a été débitée, l'application reçoit une nouvelle licence à abonnement du serveur d'activation. Toutes les fonctions sont à nouveau accessibles. Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9. Dans ce cas, à l'échéance de la validité de la licence, les fonctionnalités de l'application sont réduites. Les bases antivirus de l'application ne sont pas actualisées.

DANS CETTE SECTION

ACTIVATION DE LA VERSION COMMERCIALE

Pour activer la version commerciale de l'application à l'aide du code d'activation, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Sélectionnez **Options** → **Saisie du code**.

   L'écran d'activation de Kaspersky Mobile Security 9 s'ouvre.

5. Saisissez le code dans les 4 champs contigus. Le code d'activation est composé de lettres en alphabet latin et de chiffres et n'est pas sensible à la casse. Une fois le code d'activation saisi, choisissez l'option **Options** → **Activer** (cf. ill. ci-après).

Figure 1. Activation de la version commerciale de l'application

6. Confirmez la connexion à Internet en cliquant sur **Oui**.

7. Sélectionnez le point d'accès pour la connexion au serveur d'activation de Kaspersky Lab.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées sur l'écran.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société où vous avez acheté le code d'activation de Kaspersky Mobile Security 9.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

8. Passez à la saisie du code secret (cf. section "Saisie du code secret" à la page 24).

ACTIVATION DE L'ABONNEMENT A KASPERSKY MOBILE SECURITY 9

L'activation de l'abonnement requiert l'existence d'une connexion à Internet sur l'appareil.

Pour activer l'abonnement à Kaspersky Mobile Security 9, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Sélectionnez **Options** → **Achat rapide** (cf. ill. ci-après).

Figure 2. Activation de l'abonnement

   L'écran d'activation de Kaspersky Mobile Security 9 s'ouvre.

5. Pour confirmer l'activation de l'abonnement à Kaspersky Mobile Security 9, appuyez sur **Oui**.
6. Sélectionnez le point d'accès via lequel l'application va se connecter au serveur d'activation de Kaspersky Lab, puis cliquez sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement est accessible, alors les conditions générales de l'abonnement sont présentées.

   Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode d'activation de l'application.

7. Lisez les conditions générales de l'abonnement et si vous les acceptez, cliquez sur **Oui**.

   L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9 vous en prévient lorsque l'abonnement est activé.

   Si le solde de votre compte n'est pas suffisant pour envoyer le message SMS payant, l'activation de l'abonnement est annulée.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

   Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Non**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir le mode d'activation de l'application.

8. Passez à la saisie du code secret (cf. section "Saisie du code secret" à la page 24).

ACHAT DU CODE D'ACTIVATION EN LIGNE

Pour acheter le code d'activation de l'application en ligne, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Sélectionnez **Options** → **Acheter en ligne**.

   L'écran **Acheter en ligne** s'ouvre.

5. Appuyez sur **Ouvrir** (cf. ill. ci-dessous).

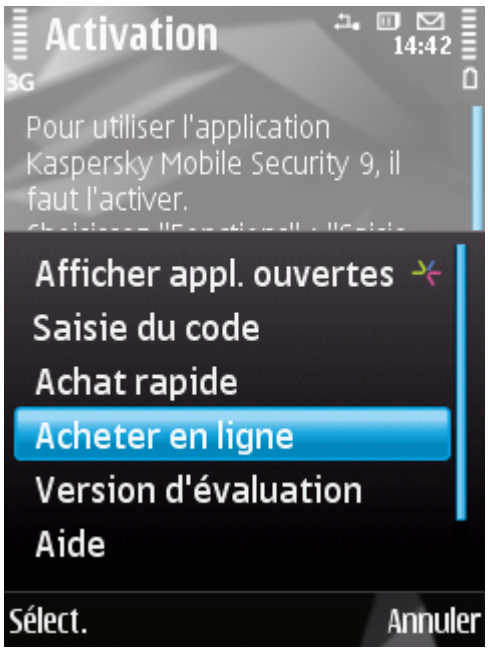

Figure 3. Achat du code d'activation en ligne

Le site Web de Kaspersky Lab pour les appareils mobiles s'ouvre. Vous pouvez y commander le renouvellement de la licence.

6. Suivez les instructions.

7. Dès que vous avez terminé l'achat du code d'activation, passez à l'activation commerciale de l'application (cf. section "Activation de la version commerciale" à la page 19).

ACTIVATION DE LA VERSION D'EVALUATION

Pour activer la version d'évaluation de Kaspersky Mobile Security 9, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.

2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Sélectionnez **Options** → **Version d'évaluation** (cf. ill. ci-après).

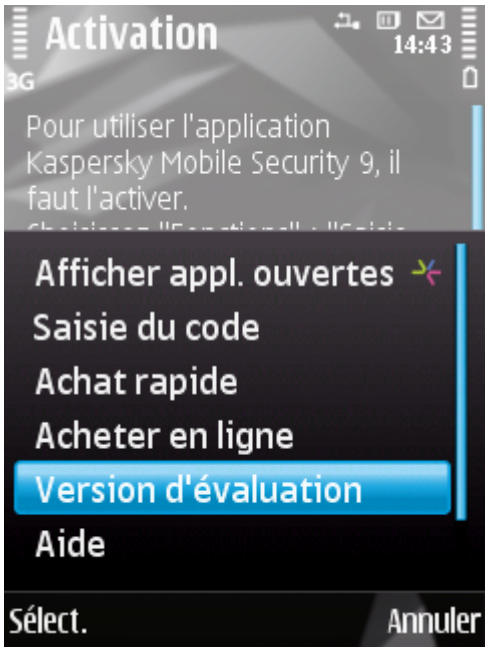

Figure 4. Activation de la version d'évaluation de l'application

5. Confirmez la connexion à Internet en cliquant sur **Oui**.

6. Sélectionnez le point d'accès pour la connexion au serveur, puis appuyez sur **OK**.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

7. Passez à la saisie du code secret (cf. section "Saisie du code secret" à la page 24).

SAISIE DU CODE SECRET

Vous serez invité à saisir le code secret de l'application après son lancement. *Le code secret de l'application* permet d'éviter l'accès non autorisé aux paramètres de l'application.

Vous pourrez modifier ultérieurement le code secret de l'application définit.

Kaspersky Mobile Security 9 demande le code secret dans les cas suivants :

- Pour accéder à l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Localisation, Contacts personnels ;
- Pour supprimer l'application.

Le code secret de l'application est composé de chiffres. Le nombre minimal de chiffres est 4.

Si vous avez oublié le code secret, vous pouvez le restaurer (cf. section "Restauration du code secret" à la page 25). Pour ce faire, il faut d'abord activer la fonction de restauration du code secret (cf. section "Activation de la fonction de restauration du code secret" à la page 24).

Pour saisir le code secret, procédez comme suit :

1. Apres l'activation de l'application dans la zone **Saisissez le nouveau code**, tapez les chiffres de votre code.

   La robustesse du code saisi est vérifiée automatiquement.

   Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche et l'application demande une confirmation. Pour utiliser le code, cliquez sur **Oui**. Pour définir un nouveau code, cliquez sur **Non**.

2. Tapez de nouveau ce code dans la zone **Confirmer**.

3. Appuyez sur **OK**.

   Le code secret sera sauvegardé.

ACTIVATION DE LA FONCTION DE RESTAURATION DU CODE SECRET

Après la première activation, vous pouvez activer l'option de restauration du code secret de l'application. Alors par la suite, vous allez pouvoir restaurer le code secret oublié de l'application.

Si vous avez refusé l'activation de cette fonction après la première activation de l'application, vous pouvez l'activer après la réinstallation de Kaspersky Mobile Security 9 sur l'appareil.

Vous pouvez restaurer le code secret de l'application (cf. section "Restauration du code secret" à la page 25), uniquement si la fonction de restauration du code secret est activée. Si vous avez oublié le mot de passe et la fonction de restauration du code secret a été désactivée, il est impossible d'administrer les fonctions de Kaspersky Mobile Security 9, ainsi que d'obtenir l'accès aux fichiers cryptés et de supprimer l'application.

Pour activer la possibilité de restaurer le code secret, procédez comme suit :

1. Après la saisie du code secret de l'application, confirmez l'activation de la fonction de restauration du code secret, en cliquant sur **Oui**.

2. Saisissez l'adresse du courrier électronique dans le champ **Votre ad. courr. élec** et cliquez sur **OK**.

   L'adresse saisie sera utilisée lors de la restauration du code secret.

   L'application établira une connexion Internet avec le serveur de restauration du code secret, enverra les informations saisies et activera la fonction de restauration du code secret.

MISE A JOUR DES BASES DU PROGRAMME

Kaspersky Mobile Security 9 recherche les menaces à l'aide des bases antivirus de l'application qui contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les moyens de les neutraliser. On y retrouve également les descriptions d'autres objets indésirables. Il se peut que les bases antivirus livrées avec Kaspersky Mobile Security 9 soient dépassées au moment de l'installation.

Il est conseillé d'actualiser les bases antivirus dès après l'installation de l'application.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur Internet.

- *Pour lancer manuellement la mise à jour des bases manuellement, procédez comme suit :*

  1. Sélectionnez **Antivirus**, choisissez l'option **Mise à jour**.

     L'écran **Mise à jour** s'ouvre.

  2. Sélectionnez l'option **Mise à jour**.

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

RECHERCHE DE VIRUS SUR L'APPAREIL

Une fois l'application installée, il est conseillé de lancer l'analyse complète de l'appareil mobile à la recherche d'éventuels objets malveillants.

La première analyse s'opère selon les paramètres définis préalablement par les experts de Kaspersky Lab.

- *Pour lancer l'analyse complète de l'appareil, procédez comme suit :*

  1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

     L'écran **Analyse** s'ouvre.

  2. Sélectionnez l'option **Analyser tout**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez consulter les informations générales sur l'application Kaspersky Mobile Security 9 et sur ses versions.

- *Pour consulter les informations relatives à l'application,*

  sous l'onglet **Avancé**, choisissez l'option **Infos logiciel**.

SUPPRESSION DE L'APPLICATION

- *Pour supprimer Kaspersky Mobile Security 9, procédez de la manière suivante :*

  1. Déchiffrez les données sur votre appareil si elles avaient été cryptées à l'aide de Kaspersky Mobile Security 9 (cf. section "Déchiffrement des données" à la page 110).

  2. Désactivez Contacts personnels (cf. section "Présentation des modes de Contacts personnels" à la page 95).

3. Fermez Kaspersky Mobile Security 9. Pour ce faire, choisissez **Options** → **Quitter** (Cf. ill. ci-après).

Figure 5. Quitter le logiciel

4. Désinstallation de Kaspersky Mobile Security 9. Pour ce faire, exécutez les actions suivantes :

   f. Ouvrez le menu principal de l'appareil.

   g. Sélectionnez le dossier **Applications** → **Install.** (voir figure suivante).

> Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

Figure 6. Chemin d'accès aux applications installées

h. Dans la liste des applications, sélectionnez **KMS 9.0**, puis choisissez **Options** → **Désinstaller** (cf. ill. ci-après).

Figure 7. Suppression de l'application

i. Pour confirmer la suppression de l'application, cliquez sur **Oui**.

j. Saisissez le code secret puis cliquez sur **OK**.

k. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :

- Si vous souhaitez conserver les paramètres de l'application et les objets en quarantaine, cochez la case en regard des paramètres requis, puis cliquez sur **OK** (cf. ill. ci-après).

- Pour supprimer complètement une application, cliquez sur **Annuler**.

Figure 8. Liste des paramètres à sauvegarder

5. Redémarrez l'appareil pour terminer la suppression de l'application.

LICENCE DE L'APPLICATION

Cette section présente les principaux concepts liés à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le Contrat de licence est un contrat juridique entre vous et Kaspersky Lab ZAO dans lequel les conditions d'utilisation de l'application sont décrites.

Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.

Vous pouvez faire connaissance avec les conditions du Contrat de licence lors de l'installation de l'application de Kaspersky Lab.

Il est estimé que vous acceptez les conditions du Contrat de licence dans les situations suivantes :

- En ouvrant la boîte contenant le CD d'installation (uniquement si vous avez acheté l'application en boîte dans les magasins de détail ou dans les magasins de nos partenaires).
- En étant d'accord avec le texte du Contrat de licence lors de l'installation de l'application.

Si vous n'êtes pas d'accord avec les conditions du Contrat de licence, vous devez interrompre l'installation de l'application.

INFOS LICENCE

La *licence* est un droit d'utilisation de l'application octroyé pour une durée définie sur la base du Contrat de licence. La licence contient le code d'activation unique de votre copie de Kaspersky Mobile Security.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs appareils.

  Le nombre d'appareils sur lequel vous pouvez utiliser l'application est défini dans le Contrat de licence.

- Recours au service d'assistance technique de Kaspersky Lab.
- Obtention des services complets proposés par Kaspersky Lab ou par ses partenaires durant la validité de la licence.

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite à durée limitée qui permet de prendre connaissance de l'application.

  Une fois la licence d'évaluation expirée, Kaspersky Mobile Security 9 arrête de fonctionner. Pour pouvoir continuer à utiliser l'application, vous devez acheter une licence commerciale.

- *Commerciale :* licence payante à durée déterminée octroyée lors de l'achat de l'application.

  A l'issue de la validité de la licence commerciale, l'application continue à fonctionner, mais avec des fonctionnalités réduites. Vous pouvez toujours soumettre l'appareil mobile à une analyse antivirus et utiliser les autres composants de l'application, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour continuer à bénéficier de toutes les fonctionnalités de Kaspersky Mobile Security, il faut renouveler la licence commerciale.

  Il est conseillé de renouveler la durée de validité de la licence avant la date d'expiration de la licence actuelle afin de garantir la protection antivirus maximale de votre appareil mobile.

- *Commerciale avec achat rapide activé* : licence payante offrant une possibilité de renouvellement automatique ou manuel. La licence avec achat rapide activé est distribuée par les prestataires de service.

  La licence avec achat rapide possède une durée de validité limitée à 30 jours. Une fois que la validité a expiré, elle peut être renouvelée manuellement ou automatiquement. Le mode de renouvellement de la licence dépend de la législation en vigueur et de l'opérateur de téléphonie mobile. La licence avec achat rapide est renouvelée automatiquement si le paiement préalable du prestataire de service a été réalisé dans les temps.

  Lors du renouvellement de la licence avec achat rapide, le montant convenu indiqué dans les conditions générales de l'achat rapide est débit de votre compte personnel. La somme est débitée de votre compte personnel via un SMS payant envoyé au numéro du prestataire de service.

  Si la licence n'est pas renouvelée, Kaspersky Mobile Security 9 ne réalise plus la mise à jour des bases antivirus de l'application et les fonctionnalités de l'application sont limitées.

  Quand vous utilisez une licence avec achat rapide, vous pouvez activer une licence commerciale à l'aide d'un code d'activation. Dans ce cas, l'activation de l'achat rapide sera automatiquement annulée.

  Vous pouvez activer l'achat rapide si vous utilisez une licence commerciale. Si une licence à durée de validité déterminée était déjà activée au moment de l'activation de l'achat rapide, elle sera remplacée par la licence avec achat rapide.

PRÉSENTATION DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale pour Kaspersky Mobile Security. Ce code est indispensable pour activer l'application.

Le code d'activation est une suite de 20 caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

Le mode d'envoi du code d'activation dépend du mode d'achat de l'application :

- Si vous avez acheté Kaspersky Mobile Security en magasin, le code d'activation figure dans la documentation ou sur la boîte contenant le cédérom d'installation.

- Si vous avez acheté Kaspersky Mobile Security en ligne, le code d'activation figure dans la documentation présente dans la boîte contenant le cédérom d'installation.

Le décompte de la durée de validité de la licence débute à partir de l'activation de l'application. Si vous avez acheté une licence prévue pour l'utilisation de Kaspersky Mobile Security sur plusieurs appareils, le décompte de la durée de validité débute à partir de l'activation sur le premier appareil.

Si le code d'activation a été perdu ou supprimé par hasard après l'activation, contactez le Support technique de Kaspersky Lab pour le restaurer. La demande s'effectue depuis Mon Espace Personnel (cf. section "Support technique via Mon Espace Personnel" à la page 126).

Après avoir activé l'application à l'aide du code d'activation, vous recevez un *numéro de client*. Le numéro de client est un numéro d'utilisateur obligatoire pour obtenir le support technique par téléphone ou dans Mon Espace Personnel (cf. section "Support technique via Mon Espace Personnel" à la page 126).

AFFICHAGE DES INFORMATIONS DE LICENCE

Vous pouvez consulter les informations suivantes sur la licence : le numéro de licence, le type, le nombre de jours restant avant l'expiration, la date d'activation et le numéro de série de l'appareil.

Pour consulter les informations sur la licence, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Infos licence** dans l'onglet Informations (cf. ill. suivante).

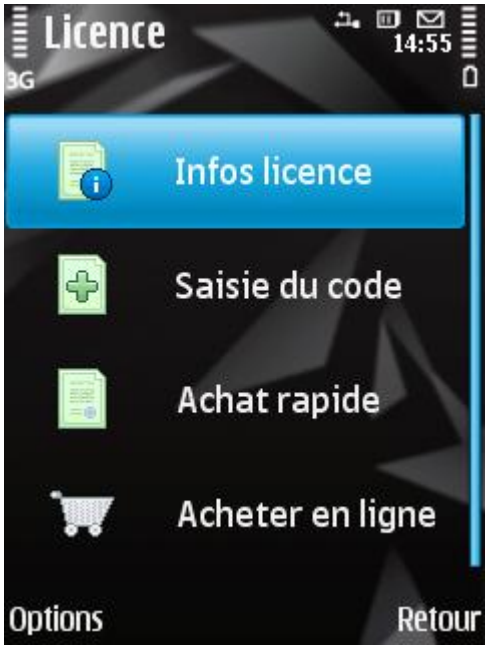

Figure 9. Affichage des informations de licence

L'écran **Infos licence** s'ouvre.

RENOUVELLEMENT DE LA LICENCE

Kaspersky Mobile Security 9 permet de renouveler la durée de validité de la licence de l'application.

Vous pouvez renouveler la licence d'une des méthodes suivantes :

- saisir le code d'activation : activation de la licence à l'aide d'un code d'activation. Le code d'activation est disponible à l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html ou chez un distributeur Kaspersky Lab.
- acheter le code d'activation en ligne. Accédez au site Web ouvert sur votre appareil mobile et achetez le code d'activation en ligne.
- s'abonner à Kaspersky Mobile Security 9. Activez l'abonnement afin de renouveler la durée de validité de la licence tous les 30 jours.

Pour pouvoir actualiser les bases de l'application sur l'appareil mobile, la connexion à Internet doit être configurée.

DANS CETTE SECTION

RENOUVELLEMENT DE LA LICENCE A L'AIDE DU CODE D'ACTIVATION

Pour renouveler la licence à l'aide du code d'activation, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Sélectionnez l'option **Saisie du code**.

   L'écran **Saisie du code** apparaît.

3. Saisissez dans l'ordre le code d'activation reçu dans les quatre champs, puis choisissez **Options** → **Activer** (cf. ill. ci-après).

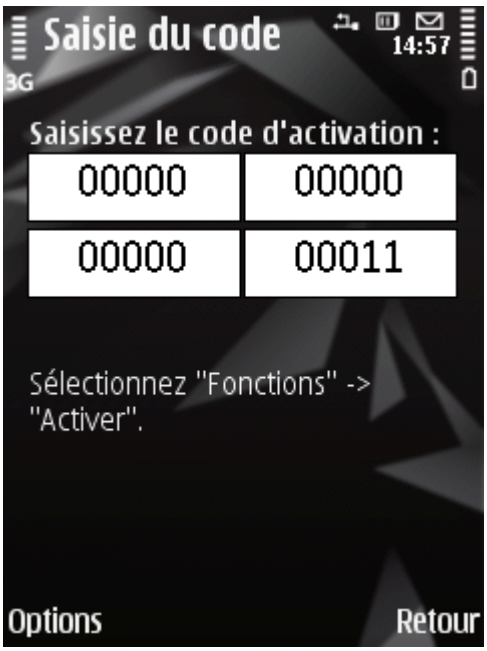

Figure 10. Renouvellement de la licence à l'aide du code d'activation

4. Si l'application demande un point d'accès, sélectionnez le type de connexion requis dans la liste proposée.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées sur l'écran.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société où vous avez acheté le code d'activation de Kaspersky Mobile Security 9.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

5. A la fin, cliquez sur **OK**.

RENOUVELLEMENT DE LA LICENCE EN LIGNE

Pour renouveler l'application en ligne, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Acheter en ligne** (cf. ill. ci-dessous).

Figure 11. Renouvellement de la licence en ligne

   L'écran **Acheter en ligne** s'ouvre.

3. Appuyez sur **Ouvrir**.

   Cette action entraîne l'ouverture d'un site Web où vous serez invité à commander le renouvellement de la licence.

   Si la durée de validité de la licence est écoulée, alors le site Web de Kaspersky Lab pour appareils mobiles s'ouvre. Vous pouvez y acheter le code d'activation en ligne.

4. Suivez les instructions.

5. Une fois que la commande du renouvellement de la licence aura été passée, saisissez le code d'activation reçu (cf. section "Renouvellement de la licence à l'aide d'un code d'activation" à la page 33).

RENOUVELLEMENT DE LA LICENCE A L'AIDE D'ACTIVATION DE L'ABONNEMENT

Vous pouvez activer l'abonnement à Kaspersky Mobile Security 9. Dans le cadre de l'abonnement, Kaspersky Mobile Security 9 renouvelle la validité de la licence tous les 30 jours. Lors de chaque renouvellement de la licence, le montant défini dans les conditions générales de l'abonnement est débité de votre compte personnel.

L'activation de l'abonnement à Kaspersky Mobile Security 9, requiert une connexion à Internet.

Pour activer l'abonnement à Kaspersky Mobile Security 9, procédez de la manière suivante :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Achat rapide** (cf. ill. ci-après).

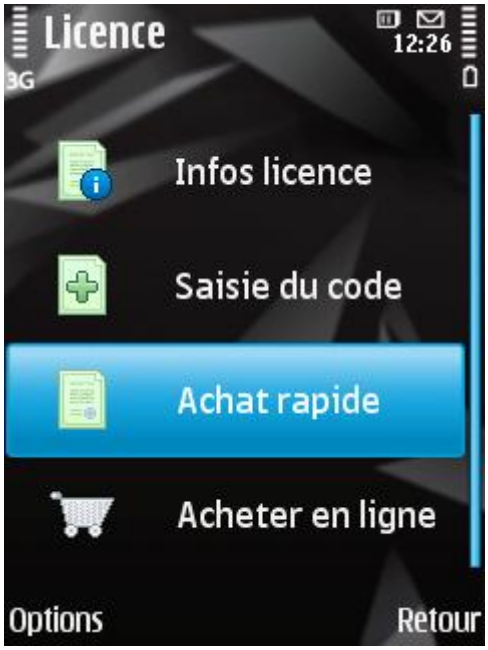

Figure 12. Activation de l'abonnement

   L'écran **Activation** s'ouvre.

3. Pour confirmer l'activation de l'abonnement à Kaspersky Mobile Security 9, appuyez sur **Oui**.

4. Sélectionnez le point d'accès via lequel l'application va se connecter au serveur d'activation de Kaspersky Lab, puis cliquez sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement est accessible, alors les conditions générales de l'abonnement sont présentées.

   Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode de renouvellement de la licence. L'activation de l'abonnement sera annulée.

5. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9 en cliquant sur **Oui**.

   L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9 vous en prévient lorsque l'abonnement est activé.

   Si le solde de votre compte n'est pas suffisant pour envoyer le message SMS payant, l'activation de l'abonnement est annulée.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

   Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Non**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir un autre mode de renouvellement de la licence.

6. A la fin, cliquez sur **OK**.

REFUS DE L'ABONNEMENT

Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9. Dans ce cas Kaspersky Mobile Security 9 ne renouvelle pas la validité de la licence tous les 30 jours. À l'échéance de la licence en cours de validité, les fonctionnalités de l'application sont réduites et les bases antivirus de l'application ne sont pas mises à jour.

Si l'abonnement est annulé, sachez que vous pouvez le reprendre (cf. section "Renouvellement de l'abonnement" à la page 38).

Pour refuser l'abonnement à Kaspersky Mobile Security 9, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Ann. abon.** (voir figure suivante).

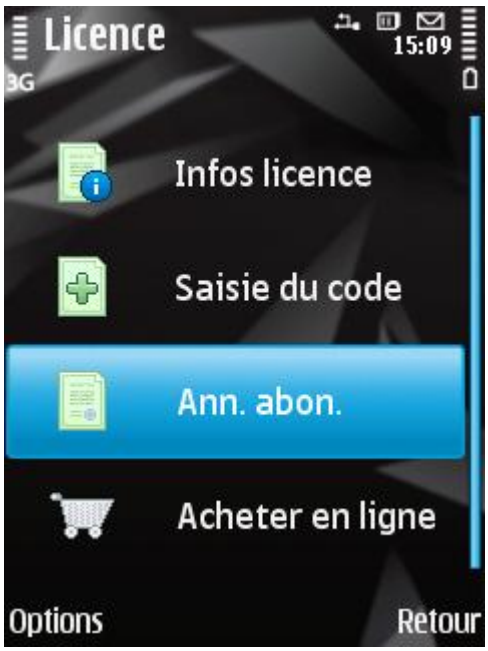

Figure 13. Refus de l'abonnement

Kaspersky Mobile Security 9 vous signale que l'abonnement a été annulé.

RENOUVELLEMENT DE L'ABONNEMENT

Si vous aviez refusé l'abonnement, vous avez la possibilité de le renouveler. Dans ce cas Kaspersky Mobile Security 9 renouvellera à nouveau la validité de la licence de l'application tous les 30 jours.

En cas de renouvellement de l'abonnement, le montant requis sera débité de votre compte personnel uniquement si la licence actuelle expire dans moins de trois jours.

Pour renouveler l'abonnement, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Achat rapide**.

Si la licence actuelle est échue, Kaspersky Mobile Security 9 propose d'activer à nouveau l'abonnement.

Si la licence actuelle est toujours valide, alors Kaspersky Mobile Security 9 renouvelle l'abonnement et quand la licence actuelle arrive à échéance, il la renouvelle tous les 30 jours.

INTERFACE DE L'APPLICATION

Cette section présente des informations sur les principaux composants de l'interface de Kaspersky Mobile Security 9.

DANS CETTE SECTION

ICONE DE PROTECTION

L'icône de la protection indique l'état de fonctionnement de l'application. Si l'icône est activée (en couleur), cela signifie que la protection est activée. Si l'icône est inactive (grise), cela indique que la protection est suspendue et que tous ses composants sont désactivés.

Par défaut, l'icône de la protection ne s'affiche pas à l'écran de l'appareil. Vous pouvez modifier les paramètres d'affichage de l'icône (cf. section "Affichage de l'icône de protection" à la page 123).

VOIR AUSSI

FENETRE D'ETAT DE LA PROTECTION

L'état des composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection.

Il existe trois états possibles pour chaque composant. Chacun d'entre eux est associé à une couleur, comme les feux de circulation. Le vert signifie que la protection de l'appareil est assurée au niveau requis. Le jaune et le rouge signalent des menaces de sécurité de nature différente. Les menaces groupent non seulement des bases antivirus dépassées, mais aussi des composants de la protection désactivés, des paramètres de base minimum de l'application etc.

La fenêtre de l'état de la protection est accessible directement après le lancement de l'application et reprend les informations suivantes :

- **Protection** : état de la protection en temps réel (cf. section "Protection en temps réel" à la page 46).

  L'icône verte de l'état indique que la protection est activée et assurée au niveau requis. Les bases antivirus de l'application sont à jour.

  L'icône jaune signale que la mise à jour des bases antivirus n'a plus eu lieu depuis quelques jours.

  L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil. Par exemple, la protection est désactivée. Il est possible que les bases antivirus n'aient pas été actualisées plus de 15 jours.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. section "Filtrage de l'activité de réseau. Pare-feu" à la page 105).

L'icône verte de l'état signifie que le composant est activé. Le niveau de protection du pare-feu a été sélectionné.

Une icône rouge indique que le filtrage de l'activité de réseau n'a pas lieu.

- **Antivol** : état de la protection des données en cas de vol ou de perte de l'appareil (cf. section "Protection des données en cas de perte ou de vol de l'appareil" à la page 84).

  L'icône verte signifie que les fonctions d'Antivol dont le nom apparaît sous l'état du composant sont activées.

  L'icône rouge indique que toutes les fonctions d'antivol sont désactivées.

- **Contacts personnels** : état de la dissimulation des informations confidentielles (cf. section "Dissimulation des informations personnelles" à la page 95).

  L'icône verte de l'état signifie que le composant est activé. Les données confidentielles sont masquées.

  L'icône jaune prévient l'utilisateur que le composant est désactivé. Les données personnelles sont visibles et peuvent être consultées.

- **Licence** : durée de validité de la licence (cf. section "Administration des licences" à la page 30).

  L'icône verte d'état indique que la licence est encore valide pendant plus de 14 jours.

  L'icône jaune indique que la licence est valide pour moins de 14 jours.

  L'icône rouge indique que la validité de la licence est écoulée.

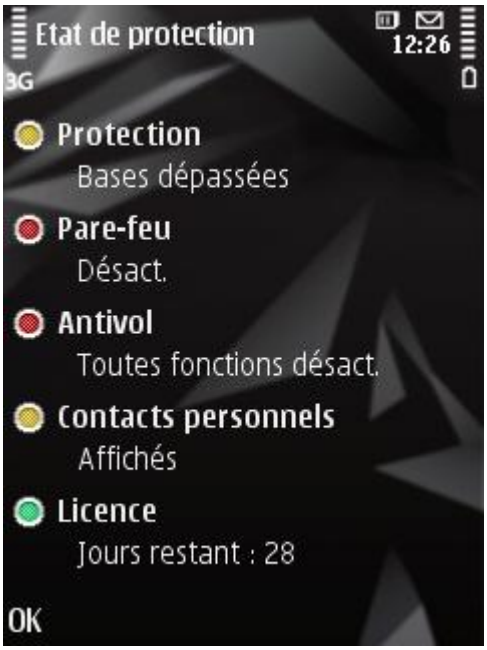

Figure 14. Fenêtre d'état de la protection

Vous pouvez également ouvrir la fenêtre d'état de la protection en sélectionnant l'option **Options** → **Etat de protection**.

Par défaut, la fenêtre de l'état de la protection s'affiche directement après le lancement de l'application. Vous pouvez modifier ses paramètres d'affichage (cf. section "Affichage de la fenêtre d'état" à la page 122).

VOIR AUSSI

ONGLETS DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et accessibles sur les onglets de l'application. Chaque onglet permet d'accéder aux paramètres du composant sélectionné et aux tâches de la protection.

Kaspersky Mobile Security 9 propose les onglets suivants :

- **Anti-Virus** : protection du système de fichiers, analyse à la demande et mise à jour des bases antivirus de l'application.
- **Contacts personnels** : masque les informations confidentielles sur l'appareil.
- **Antivol** : blocage de l'appareil et suppression des informations en cas de vol ou de perte.
- **Chiffrement** : chiffre les données stockées sur l'appareil.
- **Filtre app. /SMS** : filtrage des SMS et des appels entrants non sollicités.
- **Ctrl parental** : contrôle des appels et des SMS sortants.
- **Pare-feu** : contrôle l'activité de réseau.
- **Avancé** : paramètres généraux de l'application, informations sur l'application, sur les bases antivirus utilisées et sur la licence.

Par défaut, les onglets de l'application sont accessibles après la consultation de la fenêtre sur l'état de la protection (cf. section "Fenêtre d'état de la protection" à la page 39).

Vous pouvez naviguer entre les onglets d'une des manières suivantes :

- avec le joystick de l'appareil ou avec le stylet ;
- via le menu **Options** → **Ouvrir onglet**.

MENU DE L'APPLICATION

Le menu de l'application permet de passer à l'exécution des principales actions. Le menu contient les options suivantes (cf. ill. ci-après) :

- **Sélection** : sélection de la fonction, de l'instruction ou du paramètre.
- **Ouvrir l'onglet** : passage à la sélection du composant de l'application.
- **Etat de protection** : ouverture de la fenêtre de l'état de la protection.
- **Aide** : affichage de l'aide contextuelle de Kaspersky Mobile Security 9.
- **Infos logiciel** : affichage de l'écran reprenant les informations sur l'application.
- **Quitter** : arrêt de Kaspersky Mobile Security 9.

Figure 15. Menu de l'application

➡ *Pour ouvrir le menu de l'application,*

sélectionnez **Options**.

Pour naviguer dans le menu de l'application, utilisez le joystick de l'appareil ou le stylet.

DEMARRAGE DU LOGICIEL

Pour lancer Kaspersky Mobile Security 9, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Saisissez le code secret puis cliquez sur **OK**.

La fenêtre d'état de la protection de Kaspersky Mobile Security 9 (cf. section "Fenêtre d'état de la protection" à la page 39) apparaît à l'écran. Pour passer aux fonctions de l'application, appuyez sur **OK**.

RESTAURATION DU CODE SECRET

Vous pouvez restaurer le code secret uniquement si la fonction de restauration du code secret (cf. section "Activation de la fonction de restauration du code secret" à la page 24) avait été activée.

Pour restaurer le code secret de l'application, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran Kaspersky Mobile Security 9.0 s'ouvre.

4. Cliquez sur **Annuler**.

   Un message proposant de passer à la restauration du code secret apparaîtra à l'écran.

5. Passez à la restauration du code secret, en cliquant sur **Oui**.

   Les informations suivantes seront affichées :

   - site Web de Kaspersky Lab pour restaurer le code secret ;
   - code d'indentification de l'appareil.

6. Passez au site web http://mobile.kaspersky.com/recover-code pour restaurer le code secret.
7. Saisissez les informations suivantes dans les champs correspondants :

   - adresse du courrier électronique que vous avez désigné auparavant pour restaurer le code secret ;
   - code d'indentification de l'appareil.

   Finalement, le code de restauration sera envoyé à l'adresse du courrier électronique que vous avez indiqué.

8. A l'écran de l'application, cliquez sur **Oui** et saisissez le code de restauration obtenu.
9. Saisissez un nouveau code secret de l'application. Pour ce faire, saisissez successivement le nouveau code secret dans les champs **Saisissez le nouveau code** et **Confirmation du code**.
10. Appuyez sur **OK**.

PROTECTION DU SYSTEME DE FICHIERS

La section présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. La section explique aussi comment activer / suspendre la protection et la configurer.

DANS CETTE SECTION

PRESENTATION DE LA PROTECTION

La protection est lancée en même temps que le système d'exploitation et se trouve en permanence dans la mémoire vive de l'appareil. La protection analyse tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. La protection analyse chaque fichier au moment où vous essayez de l'accéder.
2. La protection analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparant aux bases antivirus utilisées par le logiciel. Les bases antivirus de l'application contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.
3. Après l'analyse, la Protection agit en fonction de ses résultats :
   - quand du code malveillant est découvert dans le fichier, la protection le bloque et agit conformément aux paramètres définis ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Les informations sur les résultats du fonctionnement de la protection sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

L'ACTIVATION / LA DESACTIVATION DE LA PROTECTION

Lorsque la protection est activée, toutes les actions exécutées dans le système sont placées sous un contrôle permanent.

La protection contre les virus et les autres menaces est effectuée en utilisant les ressources de l'appareil. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

Les spécialistes de Kaspersky Lab recommandent de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

La désactivation de la protection n'affecte pas les tâches d'analyse antivirus et de mise à jour des bases antivirus de l'application.

L'état actuel de la protection est repris sur l'onglet **Antivirus** à côté de l'option de menu **Protection**.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour désactiver la protection, procédez de la manière suivante :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Pour le paramètre **Mode de protection**, sélectionnez la valeur **Act.** (cf. ill. ci-après).

Figure 16. Activation de la protection

3. Appuyez sur **Précédent** pour enregistrer les modifications.

Pour désactiver la protection, procédez de la manière suivante :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Attribuez la valeur **Désact.** au paramètre **Mode de protection**.

3. Appuyez sur **Précédent** pour enregistrer les modifications.

CONFIGURATION DE LA ZONE DE PROTECTION

Kaspersky Mobile Security 9 analyse par défaut les fichiers de tous les types. Vous pouvez sélectionner les types de fichiers qui seront soumis à la recherche d'éventuels objets malveillants par Kaspersky Mobile Security 9 lors du fonctionnement du composant Protection.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour sélectionner le type d'objet à analyser, procédez comme suit :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables** : analyse uniquement les fichiers exécutables des applications (par exemple, les fichiers aux formats EXE, SIS, MDL, APP).

Figure 17. Sélection des objets à analyser

3. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9 met les objets malveillants découverts en quarantaine. Vous pouvez sélectionner l'action que Kaspersky Mobile Security 9 exécute sur l'objet malveillant découvert.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer la réponse du logiciel en présence d'un objet malveillant découvert, procédez de la manière suivante (cf. ill. ci-après) :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Définissez l'action que l'application exécutera en cas de découverte d'un objet malveillant. Pour ce faire, attribuez une valeur au paramètre **Action Anti-Virus** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

Figure 18. Réponse de l'application sur l'objet malveillant

3. Appuyez sur **OK** pour enregistrer les modifications.

RESTAURATION DES PARAMETRES DE PROTECTION PAR DEFAUT

La première fois que vous accédez à l'application, ses paramètres installés par défaut sont les paramètres recommandés par les experts de Kaspersky Lab. En cas de configuration de la protection, sachez qu'il est toujours possible de revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de protection par défaut, procédez comme suit :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez **Options** → **Restaurer**.

ANALYSE DE L'APPAREIL

Cette section présente les informations sur l'analyse de l'appareil à la demande, qui permet d'identifier et de neutraliser les menaces sur votre appareil. De plus, la section décrit comment lancer l'analyse de l'appareil, comment configurer l'analyse programmée du système de fichiers, comment sélectionner les fichiers à analyser et définir l'action de l'application en cas de détection d'un objet malveillant.

DANS CETTE SECTION

PRESENTATION DE L'ANALYSE DE L'APPAREIL

L'analyse à la demande de l'appareil permet de détecter et de neutraliser les menaces sur votre appareil. Kaspersky Mobile Security 9 est capable de réaliser une analyse complète ou partielle de l'appareil. Autrement dit, il peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier en particulier (y compris les dossiers sur les cartes mémoire).

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Mobile Security 9 analyse les fichiers, définis dans les paramètres de vérification (cf. section "Sélection du type d'objet à analyser" à la page 55).

2. Pendant la vérification, l'application analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparant aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Après l'analyse, Kaspersky Mobile Security 9 peut appliquer les actions suivantes :

   - Quand un code malveillant est découvert dans un fichier, Kaspersky Mobile Security 9 bloque le fichier et exécute l'action sélectionnée conformément aux paramètres définis (cf. section "Sélection des actions à appliquer sur des objets" à la page 57) ;

   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

L'analyse est lancée manuellement ou automatiquement selon un horaire prédéfini (cf. section "Exécution de l'analyse programmée" à la page 53).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer l'analyse complète ou partielle à la demande en mode manuel.

Pour lancer manuellement une analyse antivirus, procédez de la manière suivante :

1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

   L'écran **Analyse** s'ouvre.

2. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

   - **Analyser tout.** : analyse tout le système de fichiers de l'appareil. L'application analyse par défaut les fichiers stockés dans la mémoire de l'appareil et sur les cartes mémoire.

   - **Analyser dossier** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte mémoire. En cas de sélection de l'option **Analyser dossier**, un écran reprenant le système de fichiers de l'appareil s'ouvre. Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick. Pour lancer l'analyse d'un dossier, sélectionnez le dossier souhaité, puis choisissez **Options** →**Analyser**.

- **Analyser RAM** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.
- **Analyser msgs.** : analyse les messages reçus via SMS, MMS ou Bluetooth.

Figure 19. Sélection de la zone d'analyse

Une fois l'analyse lancée, la fenêtre du processus d'analyse affiche l'état actuel de la tâche : nombre d'objets analysés, chemin au fichier en cours d'analyse et indicateur des résultats de l'analyse en pour cent (cf. ill. ci-après).

Figure 20. Etat de l'analyse de l'appareil

Si Kaspersky Mobile Security 9 découvre un objet malveillant, il exécute l'action sélectionnée conformément aux paramètres d'analyse définis (cf. section "Sélection des actions à appliquer sur les objets identifiés" à la page 57).

Par défaut, si l'application détecte un objet malveillant, elle essaie de le réparer. Si la réparation est impossible, l'application place l'objet découvert en quarantaine.

Une fois l'analyse terminée, des statistiques générales reprenant les informations suivantes s'affichent :

- Le nombre d'objets analysés ;
- Le nombre de virus découverts, placés en quarantaine et supprimés ;
- Le nombre d'objets ignorés (par exemple, lorsque le fichier est bloqué par le système d'exploitation ou lorsque le fichier n'est pas un fichier exécutable alors que l'analyse porte uniquement sur les fichiers exécutables) ;
- L'heure de l'analyse.

Pour économiser la batterie, le rétro-éclairage de l'écran est désactivé par défaut pendant l'analyse. Vous pouvez modifier les paramètres du rétro-éclairage de l'écran (cf. section "Gestion du rétro-éclairage" à la page 121).

EXECUTION DE L'ANALYSE PROGRAMMEE

Vous pouvez configurer le lancement automatique planifié de l'analyse du système de fichiers. L'analyse est exécutée en arrière-plan. Quand un objet malveillant est détecté, l'action définie par le paramètre d'analyse est exécutée sur cet objet.

Par défaut, l'exécution d'analyse programmée est désactivée.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez une valeur aux paramètres **Analyse auto** (cf. ill. ci-après) :

   - **Désact.** : désactive le démarrage de l'analyse planifiée.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Indiquez le jour et l'heure de lancement de l'analyse. Pour ce faire, saisissez les valeurs des paramètres **Jour d'analyse** et **Heure d'analyse**.
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Indiquez l'heure de lancement de l'analyse dans le champ **Heure d'analyse**.

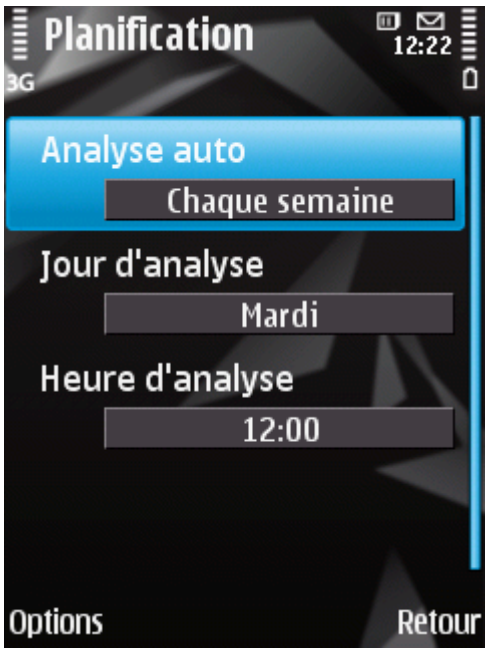

Figure 21. Programmation du lancement de l'analyse complète

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SELECTION DU TYPE D'OBJET A ANALYSER

Kaspersky Mobile Security 9 analyse par défaut tous les objets qui se trouvent sur l'appareil et sur les cartes mémoire. Pour réduire la durée de l'analyse, vous pouvez sélectionner des types d'objets à analyser, c'est-à-dire définir quels formats de fichiers seront soumis à la recherche d'un éventuel code malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour sélectionner un objet à analyser, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables** : analyse uniquement les fichiers exécutables des applications au format EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

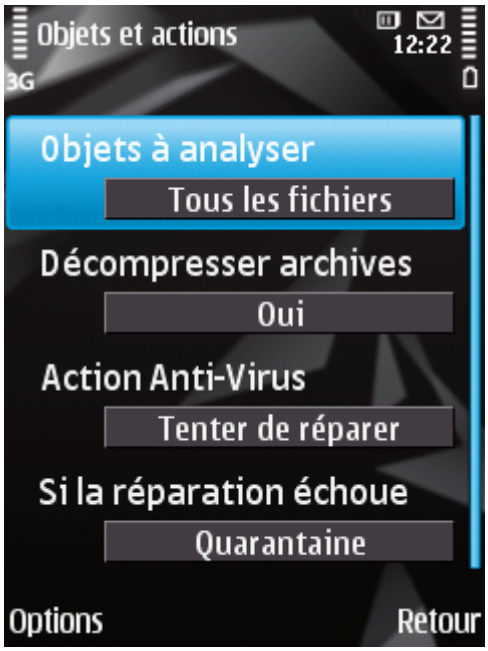

Figure 22. Sélection du type de fichiers à analyser

4. Appuyez sur **Précédent** pour enregistrer les modifications.

CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. L'application permet d'analyser les archives des formats suivants: ZIP, JAR, JAD, SIS et SISX. Pendant l'analyse, les archives sont décompressées, ce qui peut réduire sensiblement la vitesse de l'Analyse à la demande.

Vous pouvez activer / désactiver l'analyse du contenu des archives pendant l'Analyse à la demande pour détecter des codes malveillants éventuels.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour désactiver l'analyse du contenu des archives, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Attribuez au paramètre **Décompresser archives** la valeur **Non** (cf. ill. ci-dessous).

Figure 23. Configuration de l'analyse de fichiers compressés

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9 met les objets infectés découverts en quarantaine. Vous pouvez configurer les actions appliquées quand il détecte un objet malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour définir l'action que l'application exécutera sur l'objet malveillant découvert, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Définissez l'action à exécuter sur les objets malveillants. Pour ce faire, attribuez une valeur au paramètre **Action Anti-Virus** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants détectés.
   - **Confirmer** : confirme l'action auprès de l'utilisateur. En cas de découverte d'une menace, une fenêtre de confirmation de l'action s'ouvre.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).
   - **Tenter de réparer** : répare les objets malveillants. Si la réparation est impossible, l'action définie pour le paramètre **Si la réparation échoue** est exécutée.

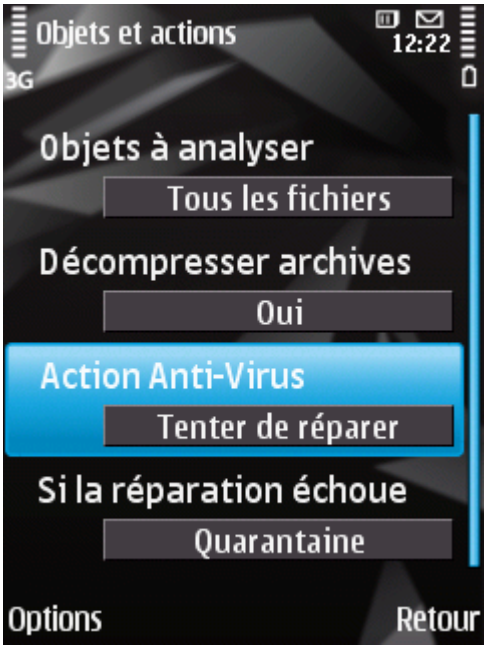

Figure 24. Sélection de l'action appliquée à un objet malveillant

4. Si vous avez choisi l'option **Tenter de réparer**, définissez la deuxième action de l'application qui sera exécutée lorsque la réparation de l'objet ne sera pas possible. Pour ce faire, attribuez une valeur au paramètre **Si la réparation échoue** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Confirmer** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

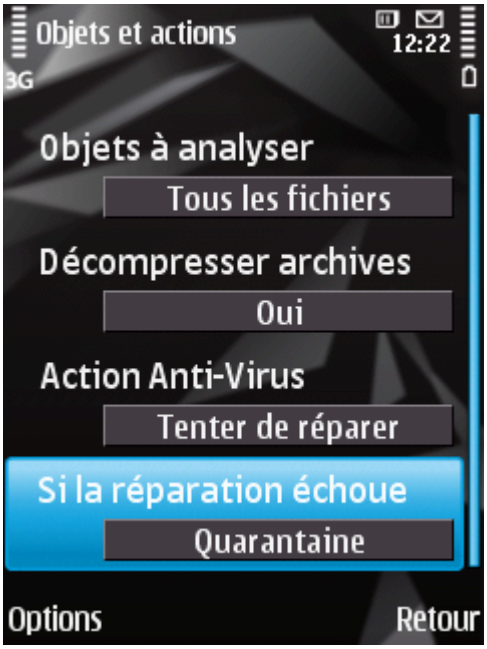

Figure 25. Sélection de l'action à exécuter sur les objets malveillants si la réparation est impossible

5. Appuyez sur **Précédent** pour enregistrer les modifications.

RESTAURATION DES PARAMETRES D'ANALYSE DE L'APPLICATION PAR DEFAUT

La première fois que vous accédez à l'application, ses paramètres installés par défaut sont les paramètres recommandés par les experts de Kaspersky Lab. En cas de configuration de l'analyse de l'appareil, sachez qu'il est toujours possible de revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de l'analyse par défaut, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Antivirus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Sélectionnez **Options** → **Restaurer**.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La section présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. De plus, elle décrit comment consulter, restaurer ou supprimer les objets malveillants stockés dans le dossier.

DANS CETTE SECTION

À PROPOS DE LA QUARANTAINE

L'application place les objets malveillants détectés en *quarantaine* dans un dossier spécial isolé pendant l'analyse de l'appareil ou pendant le fonctionnement de la protection. Les objets malveillants placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil.

Vous pouvez consulter les fichiers placés en quarantaine, les supprimer ou les restaurer.

AFFICHAGE DES OBJETS EN QUARANTAINE

Vous pouvez consulter les objets qui sont dans la quarantaine. Le nom complet de l'objet et la date à laquelle il a été découvert sont repris.

Vous pouvez également consulter des informations complémentaires sur l'objet infecté sélectionné : chemin d'accès à l'objet sur l'appareil avant sa mise en quarantaine et nom de la menace.

- *Pour afficher la liste des objets en quarantaine,*

  sélectionnez **Quarantaine** sous l'onglet **Anti-Virus**.

L'écran **Quarantaine** s'ouvre et présente la liste des objets contenus (cf. ill. ci-après).

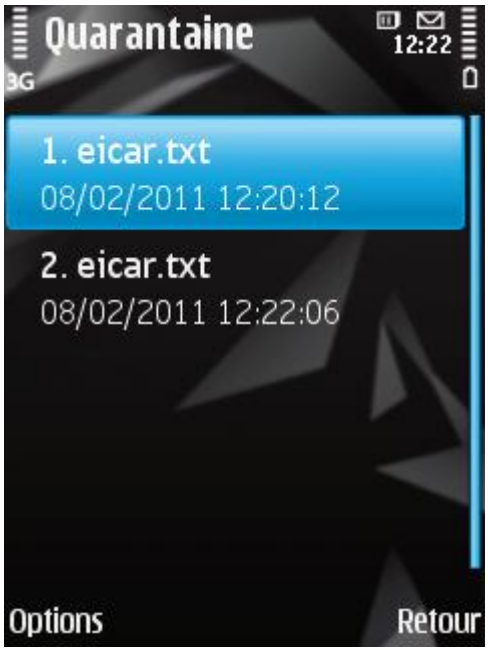

Figure 26. Liste des objets en quarantaine

- *Pour consulter les informations relatives à l'objet sélectionné,*

  choisissez le menu **Options** → **Détails**.

  L'écran affiche les informations suivantes sur le fichier : chemin d'accès au fichier selon lequel l'application l'a détecté sur l'appareil et le nom de la menace.

RESTAURATION D'OBJETS DE LA QUARANTAINE

Si vous êtes convaincu que l'objet découvert ne constitue pas une menace pour l'appareil, vous pouvez le restaurer depuis la quarantaine. L'objet restauré sera remis dans on répertoire d'origine.

- *Pour restaurer un objet depuis la quarantaine, procédez comme suit :*

  1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

     L'écran **Quarantaine** s'ouvre.

  2. Sélectionnez l'objet que vous souhaitez restaurer, puis choisissez l'option **Options** → **Restaurer**.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

Il est possible de supprimer un objet placé en quarantaine ou l'ensemble des objets placés en quarantaine.

Pour supprimer un objet de la quarantaine, procédez comme suit :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

   L'écran **Quarantaine** s'ouvre.

2. Sélectionnez l'objet que vous souhaitez supprimer, puis sélectionnez **Options** → **Supprimer**.

L'objet sélectionné sera supprimé.

Pour supprimer tous les objets de la quarantaine, procédez comme suit :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

   L'écran **Quarantaine** s'ouvre.

2. Sélectionnez **Options** → **Supprimer tout**.

Tous les objets en quarantaine seront éliminés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

Cette section présente les informations sur le Filtre des appels et SMS qui interdit la réception d'appels et des SMS non sollicités sur la base des listes noire et blanche que vous avez créées. De plus, la section indique comment sélectionner le mode Filtre des appels et SMS pour les appels et les SMS entrants, comment configurer les paramètres avancés de filtrage pour les appels et les SMS entrants et comment créer la liste noire et la liste blanche.

DANS CETTE SECTION

A PROPOS DU FILTRE DES APPELS ET SMS

Le Filtre des appels et SMS empêche la réception d'appels et de SMS non sollicités sur la base des Listes noire et blanche que vous avez créées.

Les listes contiennent les enregistrements. L'enregistrement dans chaque liste contient les informations suivantes :

- Numéro de téléphone que Filtre des appels et SMS refuse pour la liste noire et accepte pour la liste blanche.
- Type d'événement que Filtre des appels et SMS refuse pour la liste noire et accepte pour la liste blanche. Types d'informations représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Filtre des appels et SMS d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, Filtre des appels et SMS va refuser les SMS avec cette expression clé et accepter les autres SMS sans cette expression clé. S'il s'agit de la liste blanche, Filtre des appels et SMS accepte les SMS avec cette expression et refuse les SMS sans cette expression.

Filtre des appels et SMS filtre les appels et les messages selon le mode sélectionné (cf. section "A propos des Modes du Filtre des appels et SMS" à la page 64). Le Filtre des appels et SMS analyse, sur la base du mode, chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non. L'analyse se termine dès que Filtre des appels et SMS a attribué l'état de sollicité ou non au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section "Journaux du logiciel" à la page 118).

A PROPOS DES MODES DU FILTRE DES APPELS ET SMS

Le mode détermine les règles utilisées par Filtre des appels et SMS pour filtrer les appels et les SMS entrants.

Les modes de fonctionnement Filtre des appels et SMS disponibles :

- **Les deux listes** : accepte les appels et les SMS en provenance des numéros de la liste blanche et interdit ceux qui proviennent des numéros de la liste noire. Après la conversation ou la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Filtre des appels et SMS vous invitera à ajouter ce numéro sur une des listes.
- **Liste noire** : accepte tous les appels et les SMS, sauf ceux qui proviennent des numéros de la liste noire.
- **Liste blanche** : accepte uniquement les appels et les SMS en provenance des numéros de la liste blanche.
- **Désactivé** : accepte tous les appels et les SMS entrants.

Vous pouvez modifier le mode Filtre des appels et SMS (cf. section "Modification du mode Filtre des appels et SMS" à la page 64). Le mode actuel du Filtre des appels et SMS s'affiche sous l'onglet **Filtre app. /SMS** à côté du point du menu **Mode**.

MODIFICATION DU MODE FILTRE DES APPELS ET SMS

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier le mode Filtre des appels et SMS, procédez comme suit :

1. Sélectionnez **Filtre app./ SMS**, sélectionnez **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une valeur pour le paramètre **Mode Filtre app. / SMS** (cf. ill. ci-après).

Figure 27. Modification du mode Filtre des appels et SMS

3. Appuyez sur **Précédent** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Les enregistrements de la liste noire contiennent les numéros de téléphone interdits dont les appels et les SMS sont refusés par Filtre des appels et SMS. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par Filtre des appels et SMS.
- Type d'événement en provenance de ce numéro que Filtre des appels et SMS bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Filtre des appels et SMS d'identifier des SMS non sollicités (spam). Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

Filtre des appels et SMS bloquera uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste noire. Filtre des appels et SMS acceptera les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste noire.

Il est impossible d'ajouter le même numéro de téléphone avec les mêmes critères de filtrage à la liste noire et à la liste blanche.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section "Journaux du logiciel" à la page 118).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE "NOIRE"

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Filtre des appels et SMS. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter une entrée dans la liste noire Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./ SMS**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Options** → **Ajouter**.

3. Définissez les paramètres suivants (cf. ill. ci-après) :

   - **Bloquer entrants** : type d'événements en provenance du numéro de téléphone que Filtre des appels et SMS refusera pour les numéros de la liste noire :

     - **Appels et SMS :** bloque les appels et les SMS entrants.

     - **Appels seuls :** bloque uniquement les appels entrants.

     - **SMS seuls** : bloque uniquement les SMS entrants.

   - **Depuis le numéro** : numéro de téléphone pour lequel le Filtre des appels et SMS bloque les informations entrantes. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste noire. Filtre des appels et SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Filtre des appels et SMS refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

   Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cet enregistrement vide.

Figure 28. Paramètres d'un enregistrement de la liste noire

4. Appuyez sur **Retour** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez modifier les valeurs de tous les paramètres de l'entrée de la liste noire.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste noire du Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./ SMS**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis sélectionnez **Options** → **Modifier**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Bloquer entrants** : type d'événements en provenance du numéro de téléphone que Filtre des appels et SMS refusera pour les numéros de la liste noire :

     - **Appels et SMS :** bloque les appels et les SMS entrants.

     - **Appels seuls :** bloque uniquement les appels entrants.

     - **SMS seuls** : bloque uniquement les SMS entrants.

   - **Depuis le numéro** : numéro de téléphone pour lequel le Filtre des appels et SMS bloque les informations entrantes. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste noire. Filtre des appels et SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Filtre des appels et SMS refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

     Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cet enregistrement vide.

4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez supprimer ce numéro de la liste noire. Outre cela, vous pouvez purger la liste noire de Filtre des appels et SMS en supprimant tous les enregistrements qu'elle contient.

Pour supprimer un enregistrement de la liste noire du Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste, l'enregistrement à supprimer, puis sélectionnez **Options** → **Supprimer**.

Pour purger la liste noire Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste noire**.
2. L'écran **Liste noire** s'ouvre.
3. Sélectionnez **Options** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Les enregistrements de la liste blanche contiennent les numéros de téléphone autorisés dont les appels et les SMS sont acceptés par Filtre des appels et SMS. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par Filtre des appels et SMS.
- Type d'événements en provenance de ce numéro que Filtre des appels et SMS. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Filtre des appels et SMS d'identifier des SMS sains (non spam). Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

Filtre des appels et SMS accepte uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste blanche. Filtre des appels et SMS refuse les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste blanche.

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE "BLANCHE"

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Filtre des appels et SMS. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste blanche Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez **Options** → **Ajouter**.

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que Filtre des appels et SMS autorisera pour les numéros de la liste noire :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seuls :** autorise uniquement les appels entrants.
     - **SMS seuls** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone pour lequel le Filtre des appels et SMS autorise les informations entrantes. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Filtre des appels et SMS acceptera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

     Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cet enregistrement vide.

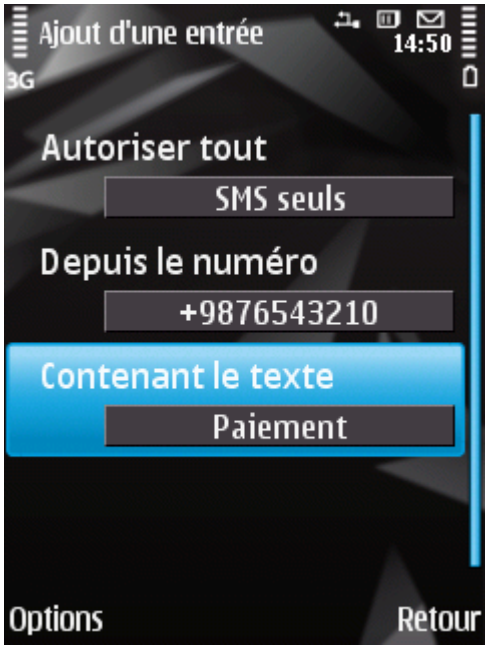

Figure 29. Paramètres d'un enregistrement de la liste blanche

4. Appuyez sur **Retour** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanches des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste blanche du Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis sélectionnez **Options** → **Modifier**.

3. Modifier les paramètres requis de l'enregistrement :

   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que Filtre des appels et SMS autorisera pour les numéros de la liste noire :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seuls :** autorise uniquement les appels entrants.
     - **SMS seuls** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone pour lequel le Filtre des appels et SMS autorise les informations entrantes. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Filtre des appels et SMS acceptera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

- **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cet enregistrement vide.

4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer une seule entrée de la liste blanche ou purger la liste.

Pour supprimer un enregistrement de la liste blanche du Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste, l'enregistrement à supprimer, puis sélectionnez **Options** → **Supprimer**.

Pour purger la liste blanche Filtre des appels et SMS, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez **Options** → **Supprimer tout**.

REACTION AUX SMS ET APPELS DE CONTACTS QUI NE FIGURENT PAS DANS LE REPERTOIRE TELEPHONIQUE

Pour le mode du Filtre des appels et SMS **Les deux listes** ou **Liste blanche**, vous pouvez configurer une action supplémentaire du Filtre des appels et SMS pour les appels et SMS des abonnés qui ne figurent pas dans les Contacts. Filtre des appels et SMS permet d'élargir la liste blanche en y introduisant les numéros des contacts.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour définir la réaction de Filtre des appels et SMS face aux numéros ne figurant pas dans le répertoire téléphonique de l'appareil, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Autoriser contacts** (cf. ill. ci-après) :

   - pour que le Filtre des appels et SMS considère les numéros du répertoire comme une liste blanche supplémentaire, cliquez sur **Oui** ;

   - pour que Filtre des appels et SMS filtre les SMS et les appels uniquement sur la base du régime défini de Filtre des appels et SMS, cliquez sur **Non**.

Figure 30. Réaction de Filtre des appels et SMS face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

3. Appuyez sur **Retour** pour enregistrer les modifications.

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Pour le mode du Filtre des appels et SMS **Les deux listes** ou **Liste noire**, vous pouvez étendre la liste noire en y incluant tous les numéros sans chiffre (contenant des lettres). Alors Filtre des appels et SMS pourra bloquer les SMS en provenance de numéros sans chiffres.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Afin de définir les réactions de Filtre des appels et SMS face aux SMS en provenance de numéros sans chiffres, procédez comme suit :

1. Sous l'onglet **Filtre app./SMS**, sélectionnez **Mode**.

   L'écran **Mode** s'ouvre.

2. Choisissez la valeur du paramètre **Non numériques** (cf. ill. ci-après) :

   - pour que le Filtre des appels et SMS supprime automatiquement les SMS provenant de numéros sans chiffre, sélectionnez la valeur **Bloquer** ;

   - pour que Filtre des appels et SMS filtre les SMS en provenance de numéros sans chiffre sur la base du mode sélectionné pour Filtre des appels et SMS, sélectionnez la valeur **Autoriser**.

Figure 31. Sélection des actions exécutées par Filtre des appels et SMS en cas de réception de SMS depuis un numéro sans chiffre.

3. Appuyez sur **Retour** pour enregistrer les modifications.

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Dans le mode **Les deux listes**, le Filtre des appels et SMS analyse les SMS entrants en les comparant à la fois à la liste noire et à la liste blanche.

Après la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Filtre des appels et SMS vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez choisir une des actions suivantes à exécuter sur le SMS (cf. ill. ci-après) :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, sélectionnez **Options** → **Ajouter à la liste noire**.

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste blanche, sélectionnez **Options** → **Ajouter à la liste blanche**.

- Pour accepter le SMS sans consigner le numéro de téléphone de l'appelant dans aucune des listes, appuyez sur **Ignorer**.

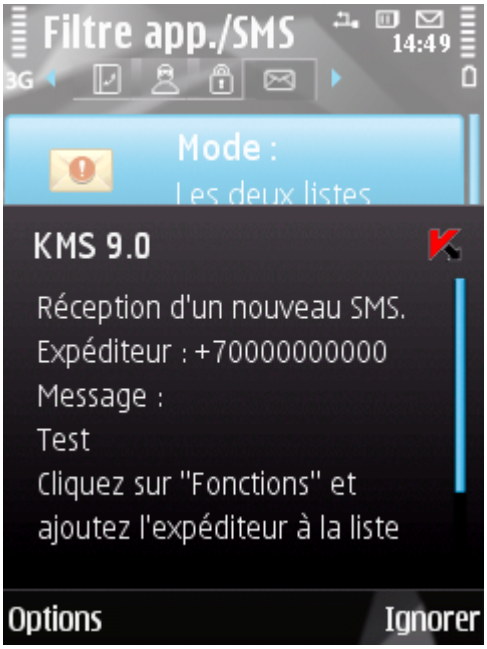

Figure 32. Notification de Filtre des appels et SMS sur le SMS reçu

Les informations sur les SMS bloqués sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Dans le mode **Les deux listes**, le Filtre des appels et SMS analyse les appels entrants en les comparant à la fois à la liste noire et à la liste blanche.

Après la réception d'un appel en provenance du numéro qui ne figure sur aucune des listes, Filtre des appels et SMS vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez choisir une des actions suivantes pour le numéro de l'appelant (cf. ill. ci-après) :

- Pour ajouter le numéro de téléphone de l'appelant à la liste noire, sélectionnez **Options** → **Ajouter à la liste noire**.

- Pour ajouter le numéro de téléphone de l'appelant à la liste blanche, sélectionnez **Options** → **Ajouter à la liste blanche**.

- Choisissez **Ignorer** si vous ne souhaitez pas consigner le numéro de l'appelant dans aucune des listes.

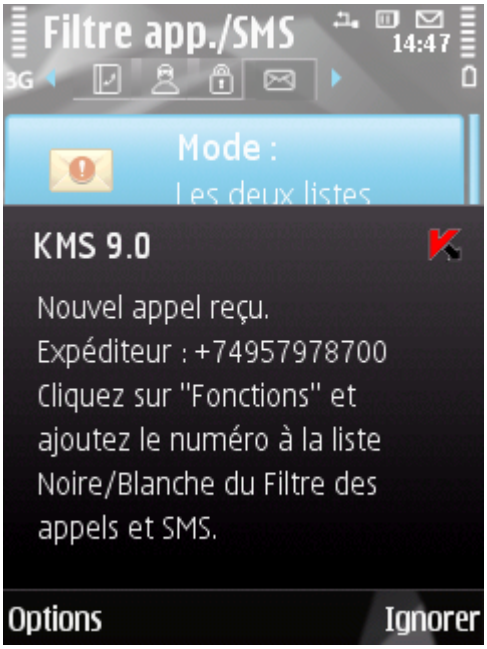

Figure 33. Notification de Filtre des appels et SMS sur l'appel reçu

Les informations sur les appels bloqués sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

RESTRICTIONS SUR LES APPELS ET LES SMS SORTANTS. CONTROLE PARENTAL

Cette section présente le composant Contrôle parental qui permet de restreindre les appels et les SMS sortants à certains numéros. Elle explique également comment composer des listes de numéros interdits ou autorisés et configurer les paramètres du Contrôle parental.

DANS CETTE SECTION

À PROPOS DU CONTROLE PARENTAL

Contrôle parental permet de contrôler les appels et les messages SMS sortants sur la base de listes noire et blanche de numéros de téléphone. Le fonctionnement du composant dépend du mode.

En mode **Liste noire**, le Contrôle parental interdit l'envoi de SMS et la réalisation d'appels vers les numéros de la liste noire. L'envoi de SMS et la réalisation d'appels vers les autres numéros est autorisée. En mode **Liste blanche**, le Contrôle parental autorise l'envoi de SMS et la réalisation d'appels uniquement vers les numéros de la liste blanche. L'envoi de SMS et la réalisation d'appels vers les autres numéros sont interdits par le Contrôle parental. En mode **Désact.**, le Contrôle parental ne contrôle pas les SMS et les appels sortants.

Le Contrôle parental interdit les SMS envoyés uniquement à l'aide des outils standards de l'appareil. Le Contrôle parental autorise l'envoi de SMS via des logiciels tiers.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

MODES DU CONTROLE PARENTAL

Le mode du Contrôle parental définit la règle selon laquelle le contrôle des SMS et des appels sortants est effectué.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Désactivé** : désactive Contrôle parental. Ne pas contrôler les SMS et les appels sortants.

  Ce mode est sélectionné par défaut.

- **Liste noire** : interdit l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste noire. Tous les autres SMS et appels sont autorisés.

- **Liste blanche** : autorise l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste blanche. Tous les autres SMS et appels sont interdits.

Vous pouvez changer le mode du Contrôle parental (cf. section "Modification du mode du Contrôle parental" à la page 77).

Le mode sélectionné de Contrôle parental apparaît sur l'onglet **Ctrl parental** à côté de l'option de menu **Mode**.

MODIFICATION DU MODE DU CONTROLE PARENTAL

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier le mode de Contrôle parental, procédez comme suit :

1. Sélectionnez **Ctrl parental**, sélectionnez **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez un des modes proposés pour Contrôle parental (cf. ill. ci-après).

Figure 34. Modification du mode du Contrôle parental

3. Appuyez sur **OK** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à Contrôle parental pour bloquer les SMS et les appels sortants. La liste reprend les numéros de téléphone vers lesquels l'envoi de SMS et la réalisation d'appels seront interdits.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE "NOIRE"

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Contrôle parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste noire de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Options** → **Ajouter**.

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
     - **Appels et SMS :** bloque les appels et les SMS sortants.
     - **Appels seuls :** bloque uniquement les appels sortants.
     - **SMS seuls** : interdit les messages SMS sortants uniquement.

- **Numéro de téléphone :** numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique).

Figure 35. Paramètres d'un enregistrement de la liste noire

4. Appuyez sur **Retour** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez modifier les valeurs de tous les paramètres de la liste noire des numéros interdits.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste noire de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis sélectionnez **Options** → **Modifier**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :

     - **Appels et SMS :** bloque les appels et les SMS sortants.

     - **Appels seuls :** bloque uniquement les appels sortants.

     - **SMS seuls** : interdit les messages SMS sortants uniquement.

   - **Numéro de téléphone :** numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique).

4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste.

Pour supprimer un enregistrement de la liste noire de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer**.

SUPPRESSION DE TOUS LES ENREGISTREMENTS DE LA LISTE NOIRE

Pour supprimer tous les enregistrements de la liste noire de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Options** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer une liste blanche sur la base de laquelle Contrôle parental autoriser l'envoi de SMS/la réalisation d'appels.

La liste reprend les numéros de téléphone vers lesquels Contrôle parental autorise l'envoi de SMS et la réalisation d'appels.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

DANS CETTE SECTION

AJOUT D'UNE ENTREE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la fois dans la liste noire et dans la liste blanche des numéros du Contrôle parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste blanche de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez **Options** → **Ajouter**.

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :

     - **Appels et SMS :** autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle parental pour l'envoi de SMS/la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique).

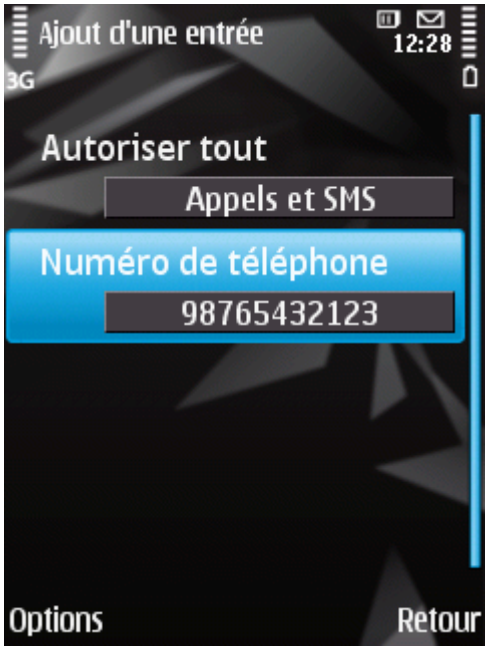

Figure 36. Paramètres d'un enregistrement de la liste blanche

4. Appuyez sur **Retour** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste blanche de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Options** → **Modifier**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :

     - **Appels et SMS :** autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle parental pour l'envoi de SMS/la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique).

4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Il est possible qu'un numéro ait été ajouté à la liste blanche par erreur. Vous pouvez supprimer ce numéro de la liste composée.

Pour supprimer un enregistrement de la liste blanche de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer**.

SUPPRESSION DE TOUTES LES ENTREES

Pour supprimer tous les enregistrements de la liste blanche de Contrôle parental, procédez comme suit :

1. Sous l'onglet **Ctrl parental**, sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Dans le menu **Options** → **Supprimer tout**.

La liste est désormais vide.

PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL

La section présente le composant Antivol, qui protège les données stockées sur l'appareil mobile contre l'accès non autorisé en cas de perte ou de vol, toute en facilitant sa recherche.

Elle explique également comment activer/désactiver les fonctions d'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la fonction Antivol depuis un autre appareil mobile.

DANS CETTE SECTION

A PROPOS DU COMPOSANT ANTIVOL

L'Antivol protège les données sur votre appareil mobile contre l'accès non autorisé.

Antivol dispose des fonctions suivantes :

- **Verrouillage** permet de verrouiller l'appareil à distance et de définir le texte qui apparaîtra à l'écran de l'appareil bloqué.
- **Suppression** permet de supprimer à distance les données personnelles de l'utilisateur (entrées dans les Contacts, SMS, galerie, calendrier, journaux, paramètres de connexion à Internet), ainsi que les données de la carte mémoire et les dossiers de la liste à supprimer.
- **SIM-Surveillance** permet de garder le numéro de téléphone en cas de remplacement de la carte SIM et de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte. Le message avec le nouveau numéro de téléphone est envoyé vers le numéro de téléphone et/ou l'adresse de la messagerie électronique que vous avez spécifiée.
- **Localisation** : permet de déterminer les coordonnées de l'appareil. Le message avec les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis le SMS spécial, ainsi que à l'adresse de la messagerie électronique.

Toutes les fonctions d'Antivol sont désactivées après l'installation de Kaspersky Mobile Security 9.

Kaspersky Mobile Security 9 permet de lancer à distance la fonction Antivol via l'envoi d'une instruction SMS depuis un autre appareil mobile (cf. section "Lancement à distance de la fonction Antivol" à la page 94).

Pour exécuter les fonctions Antivol à distance, il faudra utiliser le code secret de l'application qui a été défini à la première exécution de Kaspersky Mobile Security 9.

L'état du fonctionnement actuel de chaque fonction apparaît sur l'onglet **Antivol** à côté du nom de la fonction.

Les informations sur le fonctionnement du composant sont conservées dans le journal du composant (cf. section "Journaux de l'application" à la page 118).

VERROUILLAGE DE L'APPAREIL

Après la réception d'une instruction SMS spéciale, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données qu'il renferme. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Cette fonction ne verrouille pas l'appareil mais active uniquement la possibilité de le verrouiller à distance.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour activer la fonction de verrouillage, procédez comme suit :

1. Sous l'onglet **Antivol**, sélectionnez **Verrouillage**.

   L'écran **Verrouillage** s'ouvre.

2. Attribuez la valeur **Act.** pour le paramètre **Mode de verrouillage**.

3. Pour afficher un message à l'écran de l'appareil verrouillé, choisissez le paramètre **Texte lors du verr.** et remplissez le champ **Entrez le texte** (cf. ill. ci-après). Lorsque l'appareil est bloqué, le message "L'appareil est bloqué" s'affichera par défaut.

   Pour ne pas afficher le message, choisissez le paramètre **Texte lors du verr.** puis supprimer le contenu du champ **Entrez le texte** et appuyez sur **OK**.

Figure 37. Paramètres de la fonction Verrouillage

4. Appuyez sur **Retour** pour enregistrer les modifications.

Pour verrouiller un autre appareil, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour verrouiller l'appareil à distance, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Saisissez l'instruction **Verrouillage** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 38. Verrouillage à distance de l'appareil

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoyer**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

envoyez à un autre appareil un SMS contenant le texte `block:<code>`, où `<code>` est le code secret de l'application défini sur un autre appareil. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction SMS spéciale, la fonction Suppression permet de supprimer les informations suivantes sur l'appareil :

- données personnelles de l'utilisateur (entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet) ;
- données sur la carte mémoire ;
- données dans le dossier **C:\Data** et dans d'autres dossiers dans la liste **Dossiers à supprimer**.

Cette fonction ne supprime pas les données enregistrées sur l'appareil mais active la possibilité de le faire après la réception de l'instruction SMS.

Pour activer la fonction de suppression des données, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppression des donn.**

   L'écran **Suppression de données** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Choisissez l'option **Mode Suppr. des données** et choisissez la valeur **Act.** (cf. ill. ci-dessous).

4. Sélectionnez les données qui seront supprimées dès la réception de l'instruction SMS spéciale par l'appareil :

   - Pour supprimer les données personnelles, pour le paramètre **Supprimer données persos** attribuez la valeur **Oui** ;

- Pour supprimer les fichiers du dossier **C:\Data** et de la liste **Dossiers à supprimer**, attribuez la valeur **Oui** au paramètre **Supprimer les dossiers**.

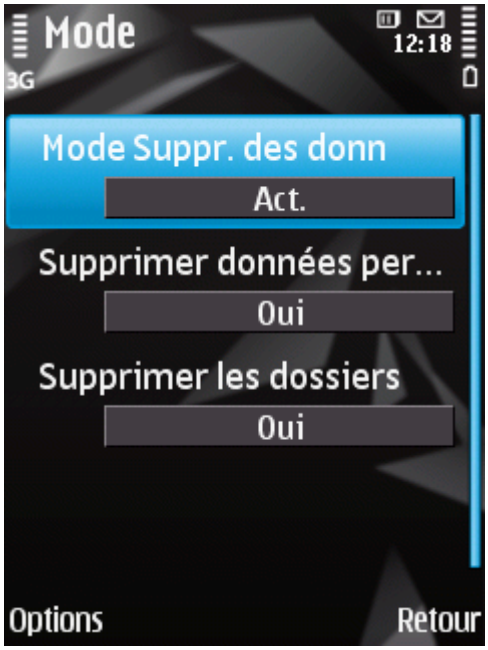

Figure 39. Paramètres de la fonction de suppression de données

5. Appuyez sur **Retour** pour enregistrer les modifications.

6. Passez à la constitution de la liste **Dossiers à supprimer** (cf. section "Composition de la liste des objets à supprimer" à la page 89).

La suppression des données personnelles de l'appareil peut être réalisée d'une des manières suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9), composez une instruction SMS et envoyez-la à votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra un SMS et les données seront supprimées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour supprimer à distance les informations de l'appareil, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Choisissez l'instruction **Suppression** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 40. Suppression de données personnelles

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoyer**.

Pour rédiger un SMS avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à un autre appareil un SMS contenant le texte `wipe:<code>` (où `<code>` est le code secret de l'application défini sur un autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception de l'instruction SMS spéciale.

Pour qu'Antivol supprime les dossiers de la liste après la réception de l'instruction SMS spéciale, assurez-vous que la valeur **Oui** est attribuée au paramètre **Supprimer les dossiers** dans le menu **Mode** de l'onglet **Antivol**.

Pour ajouter un dossier à la liste des dossiers à supprimer, procédez comme suit :

1. Sous l'onglet **Antivol**, sélectionnez **Suppression.**

   L'écran **Suppression** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Sélectionnez **Options** → **Ajouter** (cf. ill. ci-après).

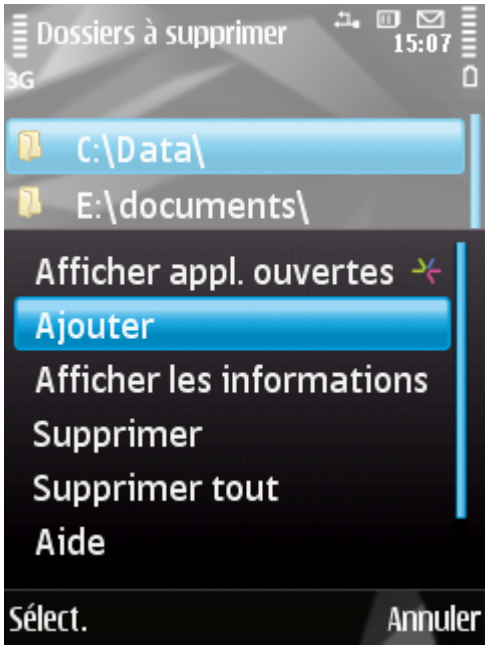

Figure 41. Ajout d'un dossier

4. Choisissez le dossier souhaité dans l'arborescence, puis cliquez sur **OK**.

   Le dossier sera ajouté à la liste.

5. Appuyez sur **Retour** pour enregistrer les modifications.

➧ *Pour supprimer un dossier de la liste, procédez comme suit :*

1. Sous l'onglet **Antivol**, sélectionnez **Suppression.**

   L'écran **Suppression** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Sélectionnez un dossier dans la liste, puis sélectionnez **Options** → **Supprimer**.

4. Pour confirmer la suppression, cliquez sur **Oui**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

SIM-Surveillance permet, en cas de remplacement de la carte SIM, d'envoyer le nouveau numéro de téléphone au numéro et/ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil.

Pour activer la fonction SIM-Surveillance et contrôler le remplacement de la carte SIM sur l'appareil, procédez comme suit :

1. Sélectionnez SIM-Surveillance dans l'onglet **Antivol**.

   L'écran **SIM-Surveillance** s'ouvre.

2. Choisissez l'option **Mode de SIM-Surveillance** et attribuez la valeur **Act**.

3. Configurez les paramètres suivants de SIM-Surveillance (cf. ill. ci-après) :

   - **Mess. sur l'ad. du cour. él.** Pour recevoir un message électronique indiquant le nouveau numéro de téléphone de votre appareil, saisissez ici une adresse électronique.

   - **SMS au numéro**. Pour recevoir automatiquement un SMS indiquant le nouveau numéro de téléphone de votre appareil, saisissez le numéro de téléphone vers lequel le message sera envoyé. Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres.

   - **Verrouiller l'appareil**. Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, sélectionnez la valeur **Oui**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret. Par défaut, le verrouillage de l'appareil est désactivé.

   - **Texte lors du verr.** Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Entrez le texte**. Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

Figure 42. Paramètres de la fonction SIM-Surveillance

4. Appuyez sur **Retour** pour enregistrer les modifications.

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Localisation détermine les coordonnées géographiques de l'appareil et les envoie par SMS ou courrier électronique à l'appareil à l'origine de la demande.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. Le récepteur GPS est activé automatiquement après la réception de l'instruction SMS spéciale. Si l'appareil se trouve dans une zone couverte par satellite, la fonction Localisation reçoit et envoie les coordonnées de l'appareil. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver sont lancées par la Localisation à intervalles réguliers.

Pour activer la fonction Localisation, procédez comme suit :

1. Sous l'onglet **Antivol**, choisissez l'option **Localisation**.

   L'écran **Localisation** s'ouvre.

2. Attribuez la valeur **Act.** au paramètre **Mode de localisation**.

3. Pour le paramètre **Mess. sur l'ad. du cour. él.** saisissez l'adresse électronique à laquelle les coordonnées géographiques de l'appareil seront envoyées (cf. ill. ci-après).

Figure 43. Paramètres de la fonction Localisation

4. Appuyez sur **Retour** pour enregistrer les modifications.

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9), composez une instruction SMS et envoyez-la à votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS, et l'application enverra les coordonnées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra à l'insu de l'utilisateur un SMS, et l'application enverra les coordonnées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour déterminer les coordonnées de l'appareil, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, le code secret sera envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Choisissez l'instruction **Localisation**, puis cliquez sur **Suivant** (cf. ill. ci-après).

Figure 44. Détermination des coordonnées de l'appareil

3. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

4. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoyer**.

Pour rédiger un SMS avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à un autre appareil un SMS contenant le texte `find:<code>` (où `<code>` est le code secret de l'application défini sur un autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Le SMS contenant les coordonnées géographiques de l'appareil sera envoyé au numéro de téléphone à l'origine de l'envoi de l'instruction SMS et à une adresse électronique, si celle-ci a été définie dans les paramètres de la fonction Localisation.

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

L'application permet d'envoyer une instruction spéciale par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Mobile Security. L'instruction SMS est envoyée sous forme d'un SMS crypté qui contient le code secret de l'application, installée sur l'autre appareil. La réception de l'instruction passera inaperçue sur l'autre appareil.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Pour envoyer une instruction SMS vers un autre appareil, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env.**

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Sélectionnez une des fonctions proposées à lancer à distance (cf. ill. ci-après) :

   - **Verrouillage** (cf. section "Verrouillage de l'appareil" à la page 85).
   - **Suppression** (cf. section "Suppression de données personnelles" à la page 87).
   - **Localisation**.
   - **Contacts personnels** (cf. section "Présentation des modes de Contacts personnels" à la page 95).

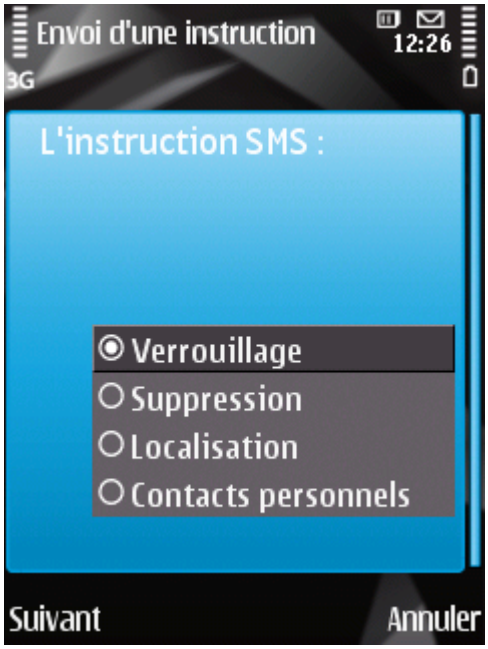

Figure 45. Lancement à distance de la fonction Antivol

La fonction doit être activée sur l'appareil qui reçoit l'instruction par SMS.

4. Cliquez sur **Suivant**.

5. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

6. Entrez le code secret spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoyer**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

La section présente le composant Contacts personnels, qui permet de dissimuler les données confidentielles de l'utilisateur.

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

Les Contacts personnels dissimulent les informations confidentielles sur la base de la Liste de contacts créée qui reprend les numéros confidentiels. Les Contacts personnels masquent les entrées dans les Contacts, les SMS entrants, sortants et brouillons, ainsi que les enregistrements dans le journal des appels pour des numéros confidentiels. Les Contacts personnels bloquent le signal de réception du SMS et le masquent dans la liste des SMS reçus. Les Contacts personnels interdisent les appels entrants d'un numéro confidentiel et l'écran n'indiquera rien au sujet de ces appels. Dans ce cas, la personne qui appelle entendra la tonalité "occupé". Il faut désactiver la dissimulation des informations confidentielles pour pouvoir consulter les appels et les SMS entrants pour la période d'activation de cette fonction. A la réactivation de la dissimulation les informations ne seront pas affichées.

Vous pouvez activer la fonction de dissimulation des informations confidentielles depuis Kaspersky Mobile Security 9 ou à distance depuis un autre appareil mobile. Vous ne pouvez désactiver la fonction de dissimulation des informations confidentielles que depuis l'application.

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. section "Journaux de l'application" à la page 118).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

Vous pouvez gérer le mode de fonctionnement de Contacts personnels. Le mode détermine si la fonction de dissimulation des données confidentielles est activée ou non.

La dissimulation est désactivée par défaut.

Les modes suivants sont prévus pour Contacts personnels :

- **Afficher** : les données confidentielles sont affichées. Les paramètres de Contacts personnels peuvent être modifiés.

- **Masquer** : les données confidentielles sont masquées. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique (cf. section "Activation automatique de la dissimulation des informations confidentielles" à la page 97) de la dissimulation des données personnelles ou son activation à distance depuis un autre appareil (cf. section "Activation de la dissimulation des informations confidentielles à distance" à la page 99).

L'état actuel de dissimulation des informations confidentielles figure sur l'onglet **Contacts personnels** à côté de l'option de menu **Mode**.

La modification du mode de fonctionnement du composant Contacts personnels peut prendre un certain temps.

MODIFICATION DU MODE DE CONTACTS PERSONNELS

Le mode du composant Contacts personnels peut être modifié d'une des manières suivantes :

- Depuis l'interface de l'application ;
- A l'aide d'un code secret lorsque l'appareil est en mode d'attente actif.

Pour modifier le mode de Contacts personnels, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Attribuez une valeur au paramètre **Mode Contacts perso.** (cf. ill. ci-après).

Figure 46. Modification du mode de Contacts personnels

3. Appuyez sur **Retour** pour enregistrer les modifications.

Pour modifier le mode du composant Contacts personnels à l'aide du code secret lorsque l'appareil est en mode d'attente actif,

saisissez dans l'ordre ***code secret#**.

Une notification apparaîtra à l'écran pour indiquer la modification du mode du composant Contacts personnels.

ACTIVATION AUTOMATIQUE DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES

Vous pouvez configurer l'activation automatique de la dissimulation des informations confidentielles après un certain temps. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Désactivez la dissimulation des informations personnelles avant de modifier les paramètres des Contacts personnels.

Pour activer automatiquement la dissimulation des informations confidentielles à l'issue d'une période déterminée, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, sélectionnez une des valeurs proposées pour le paramètre **Masquer automat**. (cf. ill. ci-après) :

   - **Sans délai**.
   - **Dans une minute**.
   - **Dans 5 minutes**.
   - **Dans 15 minutes**.
   - **Dans 1 heure**.
   - **Désact.**

Figure 47. Paramètres de lancement automatique de Contacts personnels

3. Appuyez sur **OK** pour enregistrer les modifications.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Mobile Security 9 permet d'activer à distance la dissimulation des informations confidentielles depuis un autre appareil mobile. Pour ce faire, il faut d'abord activer sur votre appareil la fonction Masquer par instruction SMS.

Pour autoriser l'activation à distance de la dissimulation des informations confidentielles, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Sélectionnez pour le paramètre **Masquer sur instr. SMS** la valeur **Oui** (cf. ill. ci-après).

Figure 48. Paramètres d'activation à distance du composant Contacts personnels

3. Appuyez sur **Retour** pour enregistrer les modifications.

Vous pouvez activer à distance la dissimulation des informations confidentielles d'une des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9), composez une instruction SMS et envoyez-la à votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS qui déclenchera la dissimulation des informations confidentielles. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra un SMS qui déclenchera la dissimulation des informations confidentielles.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile du portable utilisé pour envoyer ce SMS.

Pour activer à distance la dissimulation des informations confidentielles à l'aide d'une instruction spéciale envoyée par SMS, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Choisissez l'instruction **Contacts personnels** et cliquez sur **Suivant** (cf. ill. ci-après).

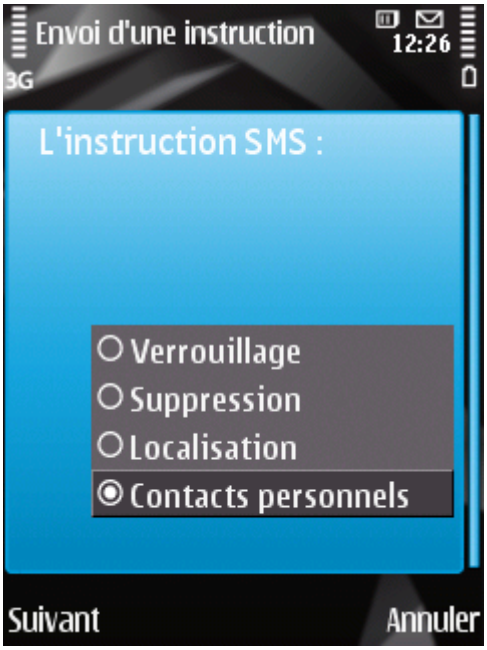

Figure 49. Lancement à distance de Contacts personnels

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoyer**.

Quand l'appareil aura reçu l'instruction par SMS, la dissimulation des informations confidentielles sera activée automatiquement.

Pour activer à distance la dissimulation des informations confidentielles avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à l'appareil un SMS contenant le texte `hide:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil récepteur). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

La liste des contacts contient les numéros confidentiels dont les informations et les événements sont masqués par le composant Contacts personnels. La liste des numéros peut être enrichie manuellement, via importation depuis les contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter un numéro dans la Liste des contacts manuellement (par exemple, +12345678) ou l'importer depuis les Contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour ajouter un enregistrement à la Liste des contacts, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Liste des contacts**.

   L'écran **Liste des contacts** apparaît.

2. Exécutez une des opérations suivantes (cf. ill. ci-après) :

   - Pour ajouter un numéro manuellement, sélectionnez **Options** → **Ajouter** → **Numéro**. Dans l'écran **Numéro** qui s'ouvre, remplissez le champ **Indiquez le téléphone**. Après avoir saisi, cliquez sur **OK**.

   - Pour ajouter un numéro depuis les Contacts, sélectionnez **Options** → **Ajouter** → **Contact**. Dans l'écran **Contacts** qui apparaît, sélectionnez le contact requis dans le répertoire via le menu **Options** → **Sélect**. Après avoir saisi, cliquez sur **OK**.

- Pour ajouter un numéro enregistré sur la carte SIM, sélectionnez **Options** → **Ajouter** → **Contacts de la carte SIM**. Sur l'écran **Contact de la carte SIM** qui apparaît, choisissez le numéro requis dans la liste des numéros de la carte SIM à l'aide de l'option **Options** → **Sélect**. Après avoir saisi, cliquez sur **OK**.

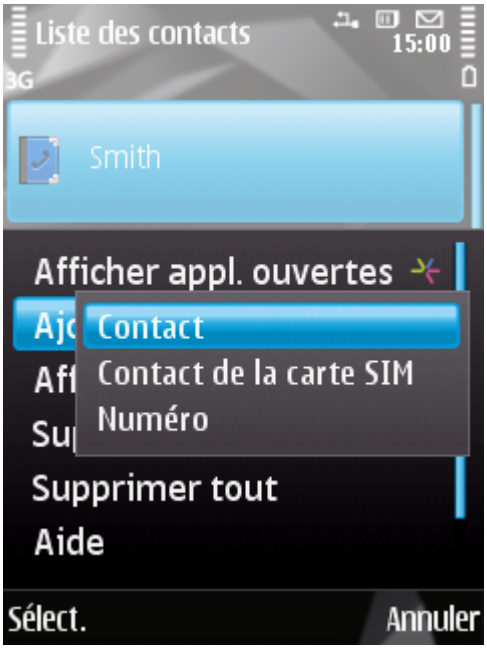

Figure 50. Ajout d'un enregistrement à la liste des contacts protégés

3. Appuyez sur **Retour** pour enregistrer les modifications.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Seuls les numéros qui ont été saisis manuellement dans la Liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans le répertoire ou dans la liste des numéros de la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour modifier le numéro dans la Liste de contacts, procédez comme suit :

1. Sélectionnez **Contacts personnels** l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez le numéro à modifier dans la Liste de contacts, puis sélectionnez **Options** → **Modifier**.

   Le numéro de téléphone du contact sélectionné apparaît à l'écran.

3. Modifiez les données dans le champ **Indiquez le téléphone**.

4. Une fois la modification terminée, cliquez sur **OK**.

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro ou effacer tout le contenu de la Liste des contacts.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour supprimer un numéro de la Liste de contacts, procédez comme suit :

1. Sélectionnez **Contacts personnels** l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez le numéro dans la liste, puis sélectionnez **Options** → **Supprimer**.

3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

Pour purger la Liste de contacts, procédez comme suit :

1. Sélectionnez **Contacts personnels** l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez **Options** → **Supprimer tout**.

3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

Les Contacts personnels permettent de dissimuler les informations suivantes pour les numéros de la Liste des contacts : contacts, SMS, entrées du journal des appels, SMS et appels entrants. Vous pouvez choisir les informations et les événements que la fonction Contacts personnels va dissimuler pour les numéros confidentiels.

Désactivez la dissimulation des informations personnelles avant de modifier les paramètres des Contacts personnels.

Pour choisir les informations et les événements à masquer pour les numéros confidentiels, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, sélectionnez l'option **Obj. à masquer**.

   L'écran **Objets à masquer** apparaît.

2. Sélectionnez les objets qui seront masqués pour les numéros confidentiels. Attribuez à chaque paramètre souhaité la valeur **Masquer** via l'option **Options** → **Modifier**. Il est possible de masquer les informations suivantes et les événements (cf. ill. ci-après) :

   - **Contacts :** masque toutes les informations relatives aux numéros confidentiels.

   - **Messages** : masquer les SMS dans les dossiers **Msgs reçus**, **Messages sortants**, **Messages envoyés** pour les numéros confidentiels.

- **Enreg. des appels** : accepte les appels en provenance des numéros confidentiels sans identifier le numéro de l'appelant et sans afficher les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).

- **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité "occupé"). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.

- **SMS entrants** : masquer la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.

Figure 51. Sélection des objets cachés

3. Appuyez sur **Retour** pour enregistrer les modifications.

FILTRAGE DE L'ACTIVITE DE RESEAU. PARE-FEU

La section présente le composant Pare-feu, qui contrôle les connexions de réseau sur votre appareil. De plus, elle décrit comment activer / désactiver le composant Pare-feu et comment sélectionner le mode de fonctionnement requis.

DANS CETTE SECTION

À PROPOS DU PARE-FEU

Le Pare-feu contrôle les connexions de réseau sur votre appareil selon le mode sélectionné. Le Pare-feu permet de désigner les connexions autorisées (par exemple, pour synchroniser avec le système d'administration distante), ainsi que les connexions interdites (par exemple, pour l'utilisation d'Internet et le téléchargement de fichiers).

Le Pare-feu est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.

Le Pare-feu permet de configurer les notifications des connexions bloquées (cf. section "Notification sur les tentatives de connexion" à la page 106).

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section "Journaux de l'application" à la page 118).

PRESENTATION DES MODES DU PARE-FEU

Vous pouvez sélectionner le mode Pare-feu pour définir les connexions autorisées et interdites. Les modes de fonctionnement Pare-feu disponibles :

- **Désact.** : autorisation de la moindre activité de réseau.
- **Les connexions entrantes sont interdites** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Les connexions sortantes des protocoles SSH, HTTP, HTTPS, IMAP, SMTP, POP3 sont autorisées** : toutes les connexions entrantes sont bloquées. La réception du courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Bloq. tout** : blocage de toute activité réseau, à l'exception de la mise à jour des bases antivirus et du renouvellement de la licence.

Vous pouvez modifier le Mode du Pare-feu (cf. section "Sélection du niveau de sécurité du Pare-feu" à la page 106). Le mode actuel est indiqué sur l'onglet **Pare-feu** à côté de l'option de menu **Mode**.

SELECTION DU NIVEAU DE SECURITE DU PARE-FEU

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour sélectionner le mode du Pare-feu, procédez comme suit :

1. Sélectionnez **Pare-feu**, choisissez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez un des modes Pare-feu proposés. Pour ce faire, mettez le curseur sur le nom du mode requis (cf. ill. ci-après).

Figure 52. Sélection du mode Pare-feu

3. Appuyez sur **OK** pour enregistrer les modifications.

NOTIFICATION SUR LES TENTATIVES DE CONNEXION

Le pare-feu bloque toutes les connexions interdites en fonction du mode sélectionné (cf. section "Sélection du niveau de sécurité du Pare-feu" à la page 106). Pour que Pare-feu vous signale les connexions bloquées sur l'appareil, configurez la réception des notifications Pare-feu.

Pour configurer la réception des notifications sur le blocage, procédez comme suit :

1. Sélectionnez **Pare-feu**, choisissez l'option **Notifications**.
2. Sélectionnez pour le paramètre **En cas de verr. de conn.** une des valeurs suivantes (cf. ill. ci-après) :
   - **Avertir** : active la réception des notifications. Le Pare-feu signale le blocage de la connexion.
   - **Ne pas avertir** : désactive la réception des notifications. Le Pare-feu ne signale pas le blocage de la connexion.

Figure 53. Configuration des notifications du Pare-feu

3. Appuyez sur **OK** pour enregistrer les modifications.

CHIFFREMENT DES DONNEES PERSONNELLES

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. De plus, la section décrit comment chiffrer et déchiffrer les dossiers sélectionnées.

DANS CETTE SECTION

À PROPOS DU CHIFFREMENT

La fonction Chiffrement permet de chiffrer les informations de la liste des dossiers à chiffrer que vous avez créée. La fonction Chiffrement repose sur une fonction de cryptage intégrée au système d'exploitation de votre appareil. La fonction Chiffrement permet de chiffrer tous les dossiers, sauf les dossiers système. Vous pouvez sélectionner pour le chiffrement des dossiers stockés dans la mémoire de l'appareil ou sur une carte mémoire. Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret défini à la première exécution de l'application.

Avant de lancer des fichiers exe exécutables depuis le dossier chiffré, il faut déchiffrer ce dossier. Pour ce faire, saisissez le code secret de l'application.

Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret. Vous pouvez définir la période (cf. section "Interdiction d'accès aux données chiffrées" à la page 111), à l'issue de laquelle l'interdiction d'accès aux dossiers chiffrés sera activée et un code secret de l'application sera nécessaire pour accéder à ces dossiers. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Le Chiffrement est désactivé après l'installation de Kaspersky Mobile Security 9.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

CHIFFREMENT DES DONNEES

Le Chiffrement permet de chiffrer un nombre quelconque de dossiers non systèmes qui se trouvent dans la mémoire de l'appareil ou sur une carte mémoire.

La liste de tous les dossiers chiffrés ou déchiffrés antérieurement est accessible dans l'écran **Chiffrement** via l'option **Liste des doss.**

Vous pouvez également chiffrer un dossier ou chiffrer directement tous les dossiers qui se trouvent dans la liste des dossiers.

- *Pour ajouter un dossier à la liste des dossiers à chiffrer pour le chiffrer, procédez comme suit :*

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des doss.**

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Options** → **Ajouter** (cf. ill. ci-après).

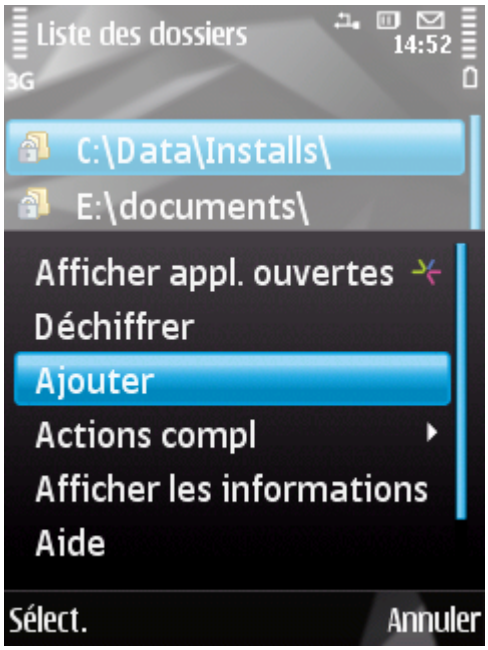

Figure 54. Chiffrement des données

   L'écran reprenant l'arborescence du système de fichiers de l'appareil apparaît.

3. Sélectionnez le dossier qu'il faut absolument chiffrer, puis lancer le processus de chiffrement du dossier sélectionné. Pour ce faire, choisissez **Options** → **Chiffrer**.

   Pour vous déplacer dans le système de fichiers, utilisez le stylet ou les boutons du joystick de votre appareil : **Haut**, **Bas** – pour vous déplacer à l'intérieur du dossier sélectionné ; **Gauche**, **Droit** – pour monter ou descendre de niveau par rapport au dossier courant.

4. Appuyez sur **OK**.

   Le dossier chiffré sera ajouté à la liste des dossiers.

Pour le dossier chiffré, le menu **Options** remplace l'option **Chiffrer** par l'option **Déchiffrer**.

Après le chiffrement, les donnée sont déchiffrées et chiffrées automatiquement lorsque vous manipulez des données depuis un dossier chiffré, lorsque vous les extrayez du dossier chiffré ou y placer de nouvelles données.

Pour chiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des doss**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Options** → **Actions compl** → **Tout chiffrer**.

3. Appuyez sur **OK**.

DECHIFFREMENT DES DONNEES

Il est possible de déchiffrer les données préalablement chiffrées (cf. section "Chiffrement de données" à la page 108). Vous pouvez déchiffrer un seul dossier ou tous les dossiers chiffrés sur l'appareil.

Pour déchiffrer un dossier chiffré, procédez comme suit :

1. Sous l'onglet **Chiffrement**, sélectionnez l'option **Liste des doss**.

   L'écran **Liste des dossiers** apparaît. Il reprend la liste de tous les dossiers chiffrés et déchiffrés antérieurement.

2. Sélectionnez dans la liste le dossier que vous voulez déchiffrer, puis choisissez **Options** → **Déchiffrer** (cf. ill. ci-après).

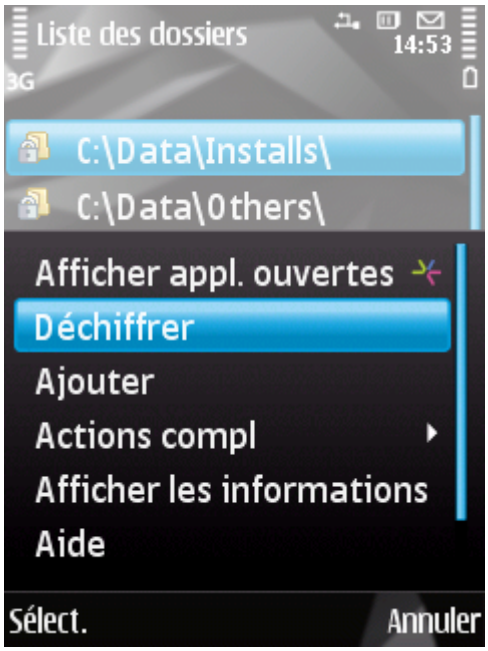

Figure 55. Déchiffrement des données

3. Cliquez sur **OK** à la fin du déchiffrement des données.

Une fois que la procédure de déchiffrement sera terminée, l'option **Déchiffrer** du menu **Options** du dossier sélectionné deviendra **Chiffre**r. Vous pouvez à nouveau utiliser le chiffrement de données (cf. section "Chiffrement de données" à la page 108).

Pour déchiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sous l'onglet **Chiffrement**, sélectionnez l'option **Liste des doss**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Options** → **Actions compl** → **Tout déchiffrer**.

3. Appuyez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le Chiffrement permet de définir la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. La fonction est activée au moment de passage de l'appareil en mode d'économie de l'énergie. Pour utiliser les informations chiffrées, il faudra saisir le code secret de l'application.

De plus, vous pouvez immédiatement bloquer l'accès aux dossiers chiffrés après leur ouverture et activer la saisie du code secret de l'application.

Pour interdire l'accès à un dossier chiffré à l'issue d'une période déterminée, procédez comme suit :

1. Sous l'onglet **Chiffrement**, choisissez l'option **Interdiction de l'accès**.

   L'écran **Int. de l'accès** s'ouvre

2. Définissez la durée après le passage de l'appareil en mode de veille pendant laquelle les données seront accessibles. Pour ce faire, choisissez une des valeurs proposées (cf. ill. ci-après) :

   - **Sans délai**.
   - **Dans une minute**.
   - **Dans 5 minutes**.
   - **Dans 15 minutes**.
   - **Dans 1 heure**.

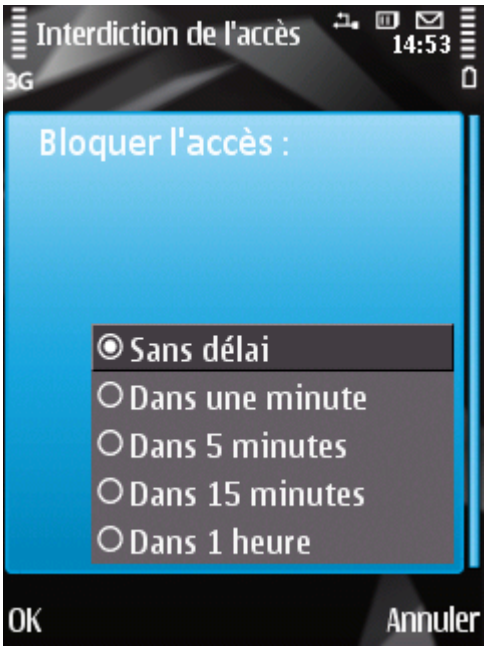

Figure 56. Blocage de l'accès aux données chiffrées

3. Appuyez sur **OK** pour enregistrer les modifications.

- *Pour interdire directement l'accès aux données chiffrées et activer la saisie du code secret,*

  appuyez simultanément sur les touches "0" et "1" de l'appareil.

MISE A JOUR DES BASES DU PROGRAMME

La section présente la mise à jour des bases anti-virus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

DANS CETTE SECTION

À PROPOS DE LA MISE A JOUR DES BASES

La recherche d'application malveillante s'opère à l'aide de base antivirus qui contiennent les descriptions de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus.

Il est conseillé d'actualiser régulièrement les bases antivirus de l'application. Si plus de 15 jours se sont écoulés depuis la dernière mise à jour, les bases antivirus de l'application sont considérées comme étant dépassées. Dans ce cas, la fiabilité de la protection sera réduite.

Kaspersky Mobile Security 9 télécharge la mise à jour des bases antivirus de l'application depuis les serveurs de mises à jour de Kaspersky Lab. Il s'agit de sites Internet spéciaux où sont hébergées les mises à jour des bases pour toutes les applications de Kaspersky Lab.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur Internet.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. Les bases antivirus de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial de Kaspersky Lab.

2. Kaspersky Mobile Security 9 exécute une des actions suivantes :

   - Si les bases antivirus de l'application que vous utilisez sont à jour, un message d'informations apparaît à l'écran.

   - Si les bases antivirus installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

     Une fois la mise à jour terminée, la connexion est automatiquement coupée. Si la connexion était déjà établie avant la mise à jour, elle reste alors disponible pour d'autres opérations.

Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres de connexion à Internet ne sont pas définis automatiquement, configurez-les (cf. section "Configuration des paramètres de connexion à Internet" à la page 116).

Vous pouvez lancer la tâche de mise à jour manuellement à n'importe quel moment, si l'appareil n'est pas occupé par l'exécution d'autres tâches ou programmer l'exécution de la mise à jour.

Si vous êtes en itinérance, vous pouvez désactiver la mise à jour des bases antivirus de Kaspersky Mobile Security 9 pour réduire les dépenses.

La date de sortie des bases est affichée dans la fenêtre d'état de la protection (cf. section "Fenêtre d'état de la protection" à la page 39). Les informations détaillées sur les bases avtivirus utilisées sont accessibles sous l'onglet **Avancé** dans l'option du menu **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page 118).

AFFICHAGE D'INFORMATIONS SUR LES BASES

Vous pouvez consulter les informations sur les bases antivirus de l'application installées : dernier lancement de la mise à jour, date de publication des bases, taille des bases et nombre d'entrées dans les bases.

- *Pour consulter les informations sur les bases antivirus existantes,*

  sous l'onglet **Avancé**, choisissez l'option **Infos des bases**.

LANCEMENT MANUEL DE LA MISE A JOUR

Vous pouvez lancer manuellement la mise à jour des bases antivirus de l'application.

- *Pour lancer manuellement la mise à jour des bases manuellement, procédez comme suit :*

  1. Sélectionnez **Antivirus**, choisissez l'option **Mise à jour**.

     L'écran **Mise à jour** s'ouvre.

  2. Sélectionnez **Mise à jour** (cf. ill. ci-après).

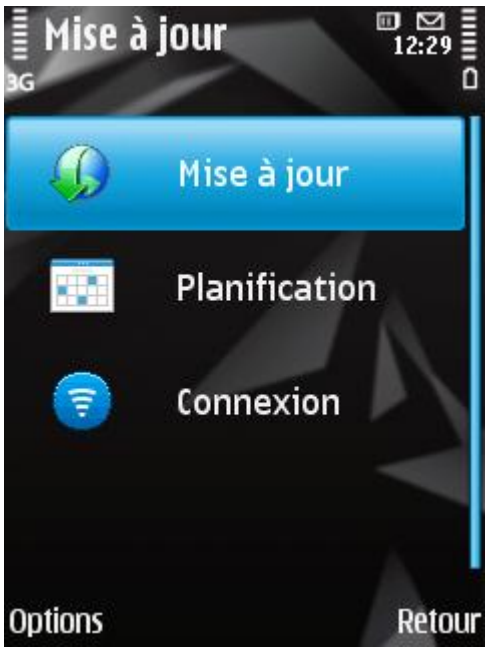

Figure 57. Lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

LANCEMENT PROGRAMME DE LA MISE A JOUR

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Pour votre confort, vous pouvez configurer l'exécution automatique de la mise à jour des bases antivirus et de programmer son exécution.

Pour exécuter une mise à jour programmée, veillez à ce que l'appareil soit allumé au moment de la mise à jour.

Vous pouvez également configurer les paramètres de mise à jour automatique si vous vous trouvez par exemple en itinérance (cf. section "Mise à jour en itinérance" à la page 116).

Pour configurer le lancement programmé de la mise à jour, procédez comme suit :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez au paramètre **Mise à jour auto** une des valeurs proposées (cf. ill. ci-après) :

   - **Désact.** : la mise à jour programmée des bases de l'application n'aura pas lieu.
   - **Chaque semaine** : actualise les bases de l'application une fois par semaine. Sélectionnez une des valeurs pour les paramètres **Jour de mise à jour** et **Heure de mise à jour**.
   - **Chaque jour** : actualise les bases chaque jour. Saisissez la valeur pour le paramètre **Heure de mise à jour**.

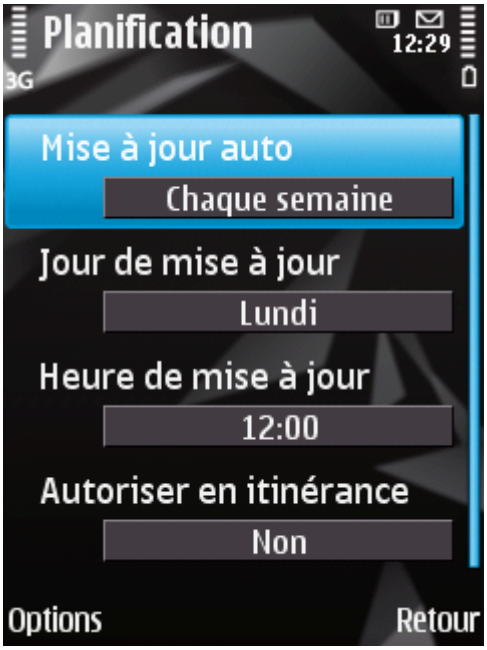

Figure 58. Programmation de la mise à jour automatique

4. Appuyez sur **Retour** pour enregistrer les modifications.

MISE A JOUR EN ITINERANCE

Vous pouvez contrôler le lancement de la mise à jour programmée en itinérance, vu que le trafic Internet est payé au tarif d'itinérance.

Si le lancement de la mise à jour programmée est interdit en itinérance, le lancement manuel de la mise à jour sera accessible en mode normal.

Pour désactiver la mise à jour programmée des bases antivirus de l'application en cas d'itinérance, procédez comme suit :

1. Sélectionnez **Antivirus**, choisissez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez la valeur **Non** au paramètre **Autoriser en itinérance** (cf. ill. ci-après).

Figure 59. Configuration des mises en jour en itinérance

4. Appuyez sur **Retour** pour enregistrer les modifications.

CONFIGURATION DES PARAMETRES DE CONNEXION A INTERNET

Pour se connecter à Internet, Kaspersky Mobile Security 9 utilise un point d'accès défini par défaut.

Les paramètres du point d'accès sont communiqués par le fournisseur.

Si Kaspersky Mobile Security 9 n'a pas défini automatiquement les paramètres de connexion, configurez-les.

Pour configurer les paramètres de connexion à Internet, procédez comme suit :

1. Sélectionnez **Antivirus**, choisissez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

2. Sélectionnez l'option **Connexion**.

3. Sélectionnez le point d'accès utilisé pour vous connecter au serveur de mise à jour. Pour ce faire, sélectionnez la valeur du paramètre **Point d'accès**, puis appuyez sur **OK** (cf. ill. ci-après).

   La liste reprendra tous les points d'accès définis sur l'appareil nomade.

Figure 60. Paramètres de connexion à Internet

4. Appuyez sur **Retour** pour enregistrer les modifications.

JOURNAUX DU LOGICIEL

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus).

DANS CETTE SECTION

À PROPOS DES JOURNAUX

Les journaux reprennent les enregistrements sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Mobile Security 9. Les enregistrements sont triés par l'heure de l'événement et classés dans l'ordre chronologique.

Il existe un journal des événements pour chaque composant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

Pour consulter les enregistrements dans le journal du composant, procédez comme suit :

1. Sous l'onglet du composant requis, choisissez l'option **Journal**.

   Le journal du composant sélectionné s'ouvre (cf. ill. ci-après).

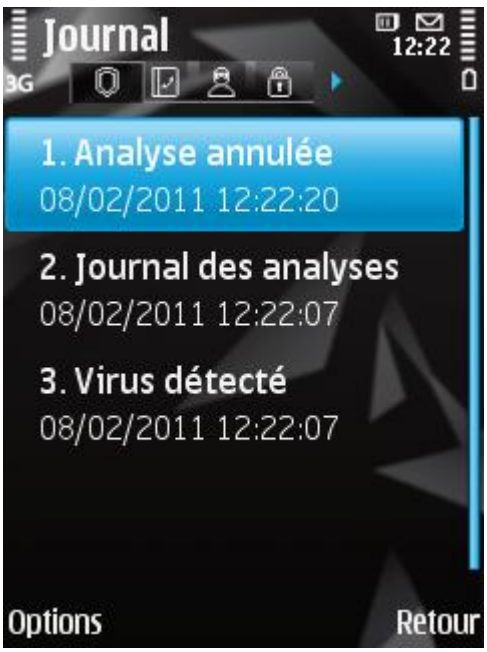

Figure 61. Journal du composant sélectionné

2. Naviguez dans le journal à l'aide du stylet ou des boutons du joystick : **Haut** et **Bas** pour consulter les événements dans le journal en cours et **Gauche** et **Droite** pour consulter les événements dans les journaux des autres composants.

Pour afficher des informations détaillées sur les enregistrements du journal,

sélectionnez l'enregistrement requis, puis choisissez **Options** → **Afficher les informations**.

SUPPRESSION D'EVENEMENTS DANS LES JOURNAUX

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Mobile Security 9 seront supprimées.

Pour supprimer tous les événements des journaux, procédez comme suit :

1. Sous l'onglet de n'importe quel composant, choisissez l'option **Journal**.

   L'écran **Journal** s'ouvre.

2. Sélectionnez **Options** → **Effacer le journal**.

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section présente les informations sur les fonctionnalités complémentaires de Kaspersky Mobile Security 9 : comment modifier le code secret, comment administrer les notifications sonores de l'application et le rétro-éclairage, et comment activer / désactiver l'affichage des astuces, de l'icône de protection ou de la fenêtre d'état de la protection.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret de l'application défini après l'installation.

Pour changer le code secret de l'application, procédez comme suit :

1. Sélectionnez **Paramètres** dans l'onglet **Avancé**.

   L'écran **Paramètres** s'ouvre.

2. Choisissez le paramètre **Modification du code**.

3. Saisissez le code actuel dans le champ **Saisissez le code**, puis cliquez sur **OK**.

4. Saisissez le nouveau code dans le champ **Saisissez le nouveau code**, puis cliquez sur **OK**.

5. Saisissez à nouveau le code dans le champ **Confirmation du code**, puis cliquez sur **OK**.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Mobile Security 9 affiche par défaut des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Mobile Security 9.

Pour configurer l'affichage des astuces, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :

   - **Afficher** : affiche l'astuce avant de configurer le paramètres de la fonction sélectionnée.
   - **Masquer** : aucune astuce n'est affichée.

3. Appuyez sur **Retour** pour enregistrer les modifications.

ADMINISTRATION DES NOTIFICATIONS SONORES

De différents événements résultent de l'exécution de l'application, par exemple, découverte d'un objet infecté ou d'un virus, expiration de la licence. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Kaspersky Mobile Security 9 active la notification sonore uniquement selon le mode défini de l'appareil.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour administrer les notifications sonores de l'application, procédez comme suit :

1. Sélectionnez **Paramètres** dans l'onglet **Avancé**.

   L'écran **Paramètres** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Notifications sonores** :

   - **Toujours** : utilise les notifications sonores quel que soit le profil sélectionné de l'utilisateur.
   - **Selon le mode** : utilise la notification sonore en fonction du mode sélectionné pour l'appareil.
   - **Désactiver** : n'utilise pas les notifications sonores.

3. Appuyez sur **OK** pour enregistrer les modifications.

CONTROLE DU RETRO-ECLAIRAGE

Quand l'application exécute une tâche de protection, l'appareil puise dans son autonomie. Pour épargner la batterie durant l'exécution des tâches, l'application permet de désactiver automatiquement le rétro-éclairage de l'écran.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer le rétro-éclairage de l'écran pendant l'exécution des tâches, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Rétro-éclairage** (cf. ill. ci-après) :

   - **Selon le mode** : utilise le rétro-éclairage en fonction du mode sélectionné pour l'appareil.
   - **Activer** : utilise toujours le rétro-éclairage de l'écran.

Figure 62. Contrôle du rétro-éclairage

3. Appuyez sur **Retour** pour enregistrer les modifications.

AFFICHAGE DE LA FENETRE D'ETAT

Vous pouvez activer ou désactiver l'affichage de la fenêtre d'état de protection au démarrage de l'application.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer l'affichage de la fenêtre d'état au démarrage de l'application, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

Sélectionnez une des valeurs proposées pour le paramètre **Fenêtre d'état** (cf. ill. ci-après) :

- **Afficher** : affiche la fenêtre d'état.
- **Masquer** : n'affiche pas la fenêtre d'état.

Figure 63. Configuration de l'affichage de la fenêtre d'état

2. Appuyez sur **Retour** pour enregistrer les modifications.

AFFICHAGE DE L'ICONE DE PROTECTION

Pour voir l'état de la protection, vous pouvez configurer l'affichage de l'icône de la protection sur l'écran de l'appareil mobile (cf. section "Icône de la protection" à la page 39).

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour modifier les paramètres d'affichage de l'icône de la protection, procédez comme suit :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Icône de protection** (cf. ill. ci-après) :

   - **Afficher partout** : affiche l'icône de la protection sur l'écran de l'appareil.
   - **Menu uniquement** : affiche l'icône de la protection uniquement lorsque le menu de l'appareil ou le menu de Kaspersky Mobile Security 9 est ouvert.
   - **Ne pas afficher** : n'affiche pas l'icône de la protection.

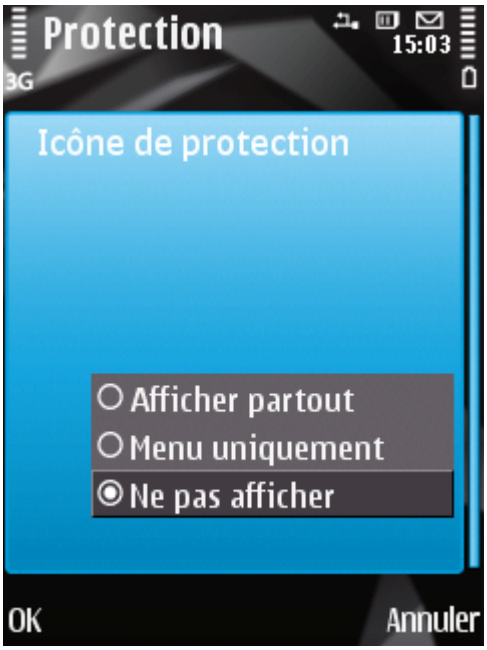

Figure 64. Paramètres d'affichage de l'icône de la protection

3. Appuyez sur **OK** pour enregistrer les modifications.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du service d'assistance technique.

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé comment résoudre votre problème dans la documentation de l'application ou dans une des sources d'informations sur l'application, veuillez contacter le Support technique de Kaspersky Lab. Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application. Si l'appareil mobile est infecté, les experts du service d'assistance technique essayeront de vous aider à supprimer les conséquences de l'exécution des programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez lire les règles d'octroi de l'assistance technique (http://support.kaspersky.com/support/rules).

Vous pouvez contacter les experts du service d'assistance technique d'une des manières suivantes :

- Via téléphone. Vous pouvez contacter les experts du service d'assistance technique en France.
- Via une demande depuis Mon Espace Personnel sur le site Web du service d'assistance technique. Cette méthode permet de contacter les experts du service d'assistance technique via un formulaire.

Afin de pouvoir obtenir l'assistance technique, vous devez être un utilisateur enregistré de la version commerciale de Kaspersky Mobile Security. Les utilisateurs des versions d'évaluation n'ont pas accès à l'assistance technique.

ASSISTANCE TECHNIQUE TÉLÉPHONIQUE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du service d'assistance Français (http://www.kaspersky.com/fr/support).

Avant de contacter le service d'assistance technique, vous devez recueillir des informations (http://support.kaspersky.com/fr/support/details) sur l'appareil mobile et les logiciels antivirus installés. Ces informations réduiront le temps de réponse de nos spécialistes.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

Mon Espace Personnel est un espace qui vous est réservé (https://my.kaspersky.com/fr) sur le site du Support technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/registration). Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel.

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au support technique et au laboratoire d'étude des virus ;
- Communiquer avec le support technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel ;
- Consulter l'historique complet de votre interaction avec le support technique.
- Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.

Écrire sa question au Service d'assistance technique

Vous pouvez envoyer une demande par voie électronique au service d'assistance technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- Type de demande ;
- Nom et numéro de version de l'application ;
- Texte de la demande ;
- Numéro de client et mot de passe ;
- Adresse de messagerie.

L'expert du service d'assistance technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

Demande électronique adressée au laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au service d'assistance technique mais au laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivantes au laboratoire d'étude des virus :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Mobile Security ne détecte aucune infection.

  Les experts du laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de découverte d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky Mobile Security considère un certain fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas.

- *Demande de description d'un programme malveillant* : vous souhaitez obtenir la description d'un virus découvert par Kaspersky Mobile Security sur la base du nom de ce virus.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Mon Espace Personnel. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application.

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'utilisateur doit avoir une licence pour activer l'application.

ANALYSE A LA DEMANDE

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

ARCHIVE

Fichier "conteneur" d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

BASES ANTIVIRUS

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît.

BLOCAGE D'UN OBJET

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

C

CODE SECRET DE L'APPLICATION

Le code secret de l'application permet d'éviter l'accès non autorisé aux paramètres de l'application et aux données protégées de l'appareil. Il est saisi par l'utilisateur à la première exécution de l'application et compte au moins quatre chiffres. Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder aux paramètres de l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Localisation, Contacts personnels ;
- Pour supprimer l'application.

D

DUREE DE LICENCE

Période de temps pendant laquelle il est possible d'exploiter toutes les caractéristiques d'une application Kaspersky Lab. A l'expiration de la licence, les fonctionnalités de l'application seront limitées. Dans ce mode sont accessibles les fonctions suivantes :

- désactiver tous les composants ;
- déchiffrer un ou plusieurs dossiers ;
- désactiver de la dissimulation des informations confidentielles ;
- désactiver la dissimulation automatique des informations confidentielles ;
- consulter le système d'aide.

DESINFECTION OU REPARATION D'OBJETS

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

L

LISTE BLANCHE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par Filtre des appels et SMS.
- Type d'événements en provenance de ce numéro que Filtre des appels et SMS. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Filtre des appels et SMS d'identifier des SMS sains (non spam). Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

LISTE NOIRE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par Filtre des appels et SMS.
- Type d'événement en provenance de ce numéro que Filtre des appels et SMS bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Filtre des appels et SMS d'identifier des SMS non sollicités (spam). Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

MASQUE DE FICHIERS

Représentation du nom et de l'extension d'un fichier moyennant des caractères génériques. Les deux caractères génériques de base utilisés dans les masques de fichier sont * et ? (où * représente une suite de caractères quelconques et ? un seul caractère). Grâce à ces caractères génériques, il est possible de désigner n'importe quel fichier. Notez que le nom et l'extension du fichier sont toujours séparés par un point.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de maintenir la protection à jour. Elle copie les bases antivirus depuis les serveurs de mises à jour de Kaspersky Lab sur l'appareil en les intégrant à l'application en mode automatique.

N

NON-NUMERIQUES

Numéro de téléphone contenant des lettres ou composé intégralement de lettres.

O

OBJET INFECTE

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l'appareil.

P

PLACER DES OBJETS EN QUARANTAINE

Méthode permettant de traiter des objets probablement infectés, en interdisant leur accès et en les déplaçant de leur position d'origine vers le dossier de quarantaine, où l'objet est enregistré sous une forme chiffrée qui annule toute menace d'infection.

Q

QUARANTAINE

Dossier spécial où sont placés tous les objets probablement infectés, détectés pendant l'analyse ou par la protection.

R

RESTAURATION D'UN OBJET

Déplacement d'un objet original depuis le dossier de quarantaine vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un autre dossier spécifié par l'utilisateur.

S

SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des SMS clairement indésirables.

SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme. Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches Anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes senior de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections anti-virus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des premiers fabricants de logiciels antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-Virus : il assure une protection complète de tous les systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. La base anti-virus de Kaspersky Lab est mise à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site Web de Kaspersky Lab:	http://www.kaspersky.com/fr
L'Encyclopédie des virus:	http://www.securelist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.com

INFORMATIONS SUR LE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

DANS CETTE SECTION

CODE DE PROGRAMMATION DIFFUSE

Le programme contient un code de programmation indépendant appartenant à d'autres éditeurs au format source ou binaire sans modification.

DANS CETTE SECTION

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

AUTRES INFORMATIONS

Informations complémentaires sur le code tiers.

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique.

Le site de CryptoEx : http://www.cryptoex.ru

INDEX

A

C

D

E

F

I

J

L

M

N

O

P

Q

R

S

V