KASPERSKY LAB

Kaspersky Anti-virus® Mobile 6.0

Guide de l'utilisateur

KASPERSKY ANTI-VIRUS® MOBILE 6.0

Guide de l'utilisateur

http://www.kaspersky.com/fr

Date de révision : Septembre 2007

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS MOBILE 6.0

Kaspersky Anti-virus® Mobile (désigné en tant que **Kaspersky Anti-virus**) est conçu pour protéger des smartphones et des Pocket PC contre les logiciels nocifs ou les messages indésirables, et dispose des fonctionnalités suivantes :

- **Mode de protection en temps réel** du système de fichiers du smartphone – interception et analyse de :
    - tous les objets entrants, transmis au moyen de connexions sans fil (port infra-rouge, Bluetooth), les messages EMS et MMS, lors de la synchronisation avec un ordinateur personnel ou du chargement de fichiers par un navigateur;
    - fichiers ouverts sur le smartphone;
    - programmes installés depuis l'interface du smartphone.
- **Analyses à la demande ou planifiée** des objets du système de fichiers, présents sur le smartphone ou sur des cartes d'extension.
- **Mise en sécurité des objets infectés** en quarantaine.
- **Mise à jour des bases anti-virus** utilisée pour détecter les applications dangereuses et supprimer les objets suspects.
- **Blocage des messages SMS et MMS indésirables**.

L'utilisateur peut personnaliser la configuration de Kaspersky Anti-virus, surveiller l'état courant de la protection et afficher le rapport d'activité de l'application.

Le logiciel possède un menu facile d'emploi et une interface conviviale.

Lors de la détection d'une application dangereuse, Kaspersky Anti-virus peut effacer l'objet infecté ou le déplacer vers la quarantaine. Le logiciel ne répare pas les objets infectés et ne fait pas de copies de sauvegarde des objets supprimés.

1.1. Spécifications matérielles et logicielles

Kaspersky Anti-virus peut s'installer sur des smartphones et des Pocket PC exploités sous l'un des systèmes d'exploitation suivants :

- Symbian 6.1, 7.0s, 8.0, 8.1, 9.1, 9.2 et Series 60 UI.
- Symbian 7.0 Series UIQ UI.
- Symbian OS 7.0 Series 80 UI.
- Microsoft Windows Mobile 2003, 2003SE.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-virus Mobile par Internet, en activant le téléchargement du programme d'installation et de la documentation en format électronique.

Vous pouvez également obtenir Kaspersky Anti-virus Mobile auprès des opérateurs de services mobiles. Pour plus de détails sur son acquisition, prenez contact avec votre opérateur mobile.

CHAPITRE 2. KASPERSKY ANTI-VIRUS FOR SYMBIAN OS SERIES 60

Ce chapitre décrit le fonctionnement de Kaspersky Anti-virus Mobile sur des smartphones exploités sous les systèmes d'exploitation Symbian version 6.1, 7.0s, 8.0, 9.1, 9.2 ou Series 60 UI. La version de l'application destinée à l'exploitation sur des smartphones sous Symbian Series UIQ est décrite avec plus de détail dans Chapitre 3 à la page 38. La version de l'application pour smartphones sous Symbian S80 est décrite au Chapitre 4 à la page 70.

2.1. Installation de Kaspersky Anti-virus

Pour installer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Copiez le paquet d'installation de l'application dans votre smartphone.
2. Exécutez l'installation (ouvrez le fichier de distribution dans votre smartphone).
3. Si un avertissement de protection est affiché, choisissez **Oui** (voir fig. 1)[1].

[1] Toutes les illustrations de ce document ont été capturées sur un smartphone modèle Nokia 6670. Sur d'autres modèles de smartphones, l'interface de l'application peut varier.

Figure 1. Avertissement de protection

4. Pour confirmer l'installation, choisissez **Oui** (voir fig. 2).

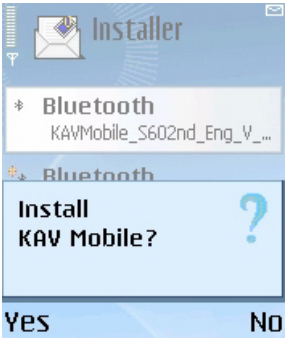

Figure 2. Confirmation de l'installation

5. Dans le menu **Options**, ouvert à la suite, sélectionnez **Installer** (voir fig. 3).

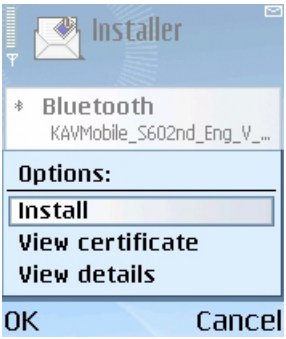

Figure 3. Menu Installer

6. Sélectionnez l'emplacement d'installation de l'application : dans la mémoire du smartphone ou sur une carte d'extension (voir fig. 4).

Figure 4. Sélection de l'emplacement d'installation de l'application

7. Si la langue du système d'exploitation n'est pas celle de Kaspersky Anti-virus, un message est affiché (voir fig. 5). Pour continuer l'installation en français, sélectionnez **Oui**.

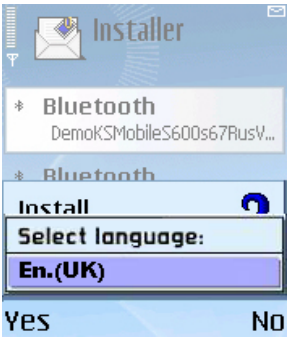

Figure 5. Sélection de la langue de l'application

8. Lisez le contrat de licence. Si vous êtes d'accord avec tous les termes, sélectionnez **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir fig. 6).

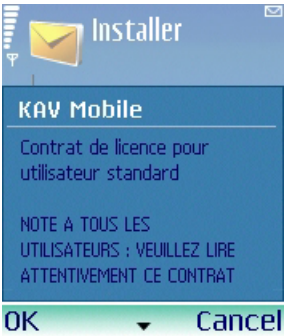

Figure 6. Contrat de licence

2.2. Utilisation de l'application

Cette section décrit la configuration de l'anti-virus et de la protection en temps réel, le filtrage des messages SMS et MMS, l'analyse anti-virus du terminal et les mises à jour de l'application.

2.2.1. Activation du logiciel

Lors de son premier démarrage, le logiciel affiche une boîte de dialogue proposant d'activer Kaspersky Anti-virus (voir fig. 7).

Figure 7. Boîte de dialogue d'activation du programme

L'activation du programme est nécessaire pour autoriser toutes les fonctionnalités de Kaspersky Anti-virus. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab.

Attention !

Une connexion GPRS est nécessaire pour activer Kaspersky Anti-virus Mobile 6.0 sur un smartphone.

Le code d'activation est composé de lettres et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus. Utilisez les boutons « Haut/Bas » pour vous déplacer aux champs précédent ou suivant.

Après avoir saisi le code d'activation, choisissez la commande **Lancer l'activation** dans le menu **Options**. L'application enverra une pétition HTTP à un serveur d'activation de Kaspersky Lab puis elle téléchargera et installera une clé de licence.

Si le code d'activation saisi s'avère être incorrect pour une raison ou une autre, le programme affiche un message correspondant.

2.2.2. Lancement de l'application

Pour lancer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Ouvrez le menu principal du smartphone.

2. Sélectionnez l'icône *KAV Mobile* et lancez l'application avec l'option **Ouvrir** dans le menu **Options**.

Après le démarrage de l'application, le smartphone affiche une fenêtre décrivant l'état des composants principaux de Kaspersky Anti-virus (voir fig. 8).

- **Protection en temps réel** – état de la protection en temps réel. Pour plus de détails, voir section 2.2.5 à la page 16.

- **Dernière analyse complète** – date et heure de la dernière analyse anti-virus du smartphone.

- **Date de la base de données** – date de publication de la base utilisée par l'application.

- **Config. Anti-Spam** – Mode de fonctionnement du composant Anti-Spam. Pour plus de détails sur les modes d'exploitation, voir section 2.2.8.1 à la page 25.

Figure 8. Fenêtre d'état des composants de l'application

Pour revenir à l'interface de l'application, appuyez sur **OK**.

2.2.3. Interface graphique utilisateur

L'interface graphique contient présente onglets :

- L'onglet **Analyse** permet d'effectuer une analyse anti-virus du smartphone, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique.
- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.
- L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de modifier les paramètres et de planifier la mise à jour.
- L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS et MMS entrants.
- L'onglet **Info** permet d'afficher les rapports d'activité des composants de l'application ; des informations générales sur l'application et la base anti-virus utilisée, ainsi que de modifier les paramètres généraux de l'application.

Pour vous déplacer d'un onglet à l'autre, utilisez le joystick de votre smartphone ou sélectionnez **Ouvrir page** dans le menu **Options** (voir fig. 9).

Figure 9. Le menu **Options**

Pour revenir à la fenêtre d'état des composants de l'application, sélectionnez **État actuel** dans le menu **Options**.

2.2.4. Paramètres généraux

Les paramètres de l'onglet **Info** dans la page **Paramètres** (voir fig. 10) permettent de configurer les caractéristiques suivantes de l'application :

- Le mode d'exploitation du composant Anti-Spam (**Config. Anti-Spam**). Sélectionnez **Activer** pour activer toutes les fonctions du composant Anti-Spam. Choisissez **Listes B/N uniquement** pour que le composant Anti-Spam utilise uniquement les listes noire et blanche. Sélectionnez **Désactiver** pour désactiver le composant Anti-Spam (reportez-vous à la section 2.2.8 à la page 24 pour plus de détails sur l'usage du composant Anti-Spam).

- Ajout du programme au dossier Favoris (**Ajouter aux Favoris**). Choisissez **Oui** pour ajouter un raccourci vers l'application dans le dossier Favoris.

  Cette caractéristique est disponible pour des smartphones sous Symbian version 9.1, 9.2 et Series 60 UI.

- Une option pour afficher l'état courant à chaque démarrage du programme (**Voir écran d'état**).

- Le nombre d'enregistrements conservés dans le rapport de l'application (**Taille rapport**).

- L'utilisation du rétro-éclairage pendant l'analyse du système de fichiers à la recherche de virus (**Rétro-éclairage**).

- L'utilisation de sons (**Activer le son**) pour communiquer certains événements (détection d'un objet infecté, informations sur l'état du programme, etc.). Sélectionnez **Actif** si vous souhaitez entendre des notifications sonores.

Figure 10. Le menu **Paramètres**

Pour modifier les valeurs des paramètres, utilisez le joystick de votre smartphone ou sélectionnez **Modifier** dans le menu **Options**.

2.2.5. Protection en temps réel des fichiers

Dans le mode de protection en temps réel, la partie résidente de Kaspersky Anti-virus reste en permanence dans la mémoire de votre smartphone, pour surveiller toutes les données ou seulement les données entrantes (en fonction des paramètres sélectionnés).

Le mode de protection en temps réel reste activé depuis le démarrage jusqu'à l'arrêt du smartphone (à moins que ce mode ne soit désactivé par configuration).

Les résultats de l'analyse sont enregistrés dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Info**.

Pour modifier la configuration de la protection en temps réel :

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).

2. Sur l'onglet **Analyse**, sélectionnez **Paramètres** (voir fig. 11).

Figure 11. Onglet **Analyse**

3. Dans le menu ouvert à la suite, configurez les paramètres nécessaires (voir fig. 12) :

Figure 12. Le menu **Paramètres**

- Activer / Désactiver la protection en temps réel (paramètre **Protection en temps réel**).

  Par défaut, dans le mode de protection en temps réel, l'application analyse toutes les données entrantes (l'option **Entrants seuls** est sélectionnée).

  Pour configurer Kaspersky Anti-virus afin d'analyser tous les fichiers entrants et le système de fichiers complet, sélectionnez **Tout analyser**.

Pour désactiver la protection en temps réel, sélectionnez **Inactif**.

- Sélectionnez les types de fichiers à analyser (option **Masque**) :

  - **Tous les fichiers** – analyse les fichiers de tous formats.

  - **Fichiers exécutables** – analyse uniquement les fichiers exécutables (par exemple, les fichiers avec extensions *.exe, *.sis, *.mdl ou *.app).

- Définissez l'action à réaliser en cas de détection d'un objet infecté (paramètre **Action anti-virus**).

  Si vous souhaitez afficher une confirmation avant d'appliquer l'action spécifiée, sélectionnez **Demander**.

  Si vous souhaitez que Kaspersky Anti-virus supprime automatiquement les messages infectés sans demander la confirmation de l'utilisateur, choisissez **Suppression auto**.

  Sélectionnez **Quarantaine** pour déplacer les objets détectés vers la quarantaine. C'est l'action par défaut utilisée pour les objets infectés.

- Activer / Désactiver l'analyse de la mémoire ROM des smartphone (paramètre **Analyser ROM**).

  En certains cas, la mémoire ROM peut être vulnérable aux applications malveillantes. Pour configurer Kaspersky Anti-virus afin d'analyser cette mémoire, sélectionnez **Oui**.

  Pour désactiver l'analyse de la ROM, sélectionnez **Non**.

- Activer / Désactiver la décompression des archives SIS, LHA et ICE (paramètre Décompresser archives). Sélectionnez **Oui** afin que Kaspersky Anti-virus décompresse les archives SIS lors de l'analyse. Si vous n'avez pas besoin de décompresser les archives SIS au cours de l'analyse, désactivez cette caractéristique avec **Non**.

- Activer / Désactiver l'analyse des nouvelles cartes mémoire (paramètre **Analyser carte**). Pour que Kaspersky Anti-virus analyse automatiquement les cartes de mémoire flash

connectées à votre smartphone, sélectionnez **Analyse auto.** Sélectionnez **Désactiver** pour annuler l'analyse automatique des cartes de mémoire flash. Pour faire en sorte que Kaspersky Anti-virus Mobile propose d'analyser chaque nouvelle carte insérée, sélectionnez **Demander**.

- Afficher / Masque l'icône de protection en temps réel (paramètre **Afficher l'icône PTR**).

  Pour que l'application affiche l'icône chaque fois que protection en temps réel est activée, sélectionnez **Toujours**. Si vous souhaitez afficher l'icône uniquement dans le menu du smartphone, sélectionnez **Menu uniquement**. Pour masquer l'icône, sélectionnez **Jamais**.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre smartphone ou sélectionnez **Modifier** dans le menu **Options**.
Par défaut, l'application utilise la configuration recommandée par les experts de Kaspersky Lab. Si vous souhaitez restaurer la configuration par défaut, dans l'onglet **Analyse** sélectionnez **Par défaut** dans le menu **Options**.

2.2.6. Analyse à la demande

Dans le mode d'*analyse à la demande*, l'application analyse votre smartphone à la recherche de logiciels nocifs à la demande de l'utilisateur ou à une heure programmée d'avance.

Kaspersky Anti-virus peut réaliser une analyse complète du système de fichiers de votre smartphone, y compris les objets conservés sur les cartes d'extension mémoire.

Les résultats de l'analyse sont enregistrés dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Info**.

La configuration de la protection en temps réel, décrite dans la section 2.2.5 à la page 16 s'applique également à l'analyse à la demande. En outre, les analyses à la demande utilisent des paramètres supplémentaires qui sont décrits plus en détail dans la suite.

2.2.6.1. Exécution manuelle d'une analyse

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

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).

2. Utilisez l'onglet **Analyse** (voir fig. 13) pour sélectionner **Tout analyser** si vous souhaitez contrôler le système de fichiers complet de votre smartphone ou **Analyser dossier** pour analyser le contenu d'un dossier individuel.

   La sélection de la commande **Analyser dossier** présente une fenêtre avec le système de fichiers du smartphone. Utilisez les boutons du joystick pour vous déplacer dans le système de fichiers. Pour lancer l'analyse d'un dossier, placez le curseur sur ce dernier puis sélectionnez **Analyser** dans le menu **Options**.

Dès que la procédure démarre, une fenêtre affiche la progression de l'analyse, avec les indicateurs en cours : nombre d'objets analysés, chemin vers l'objet en cours d'analyse et une barre progression avec le pourcentage d'objets analysés (voir fig. 13).

Figure 13. Écran de progression de l'analyse

En cas de détection d'un objet infecté, l'application propose de supprimer le fichier concerné (action **Supprimer**), de le placer en quarantaine (action **Déplacer vers quarantaine**) ou de laisser tel quel le fichier (action **Ignorer**).

Le logiciel n'affichera le choix des action possible que si le paramètre **Action anti-virus** a été définit à **Demander** (voir section 2.2.5 à la page 16 pour plus de détails).

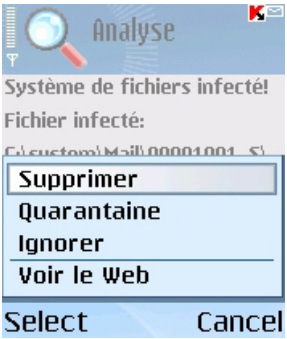

Figure 14. Notification de détection de virus

Après l'analyse, des statistiques globales sur le objets infectés /supprimés sont affichées.

Pour éviter que le rétro-éclairage ne s'éteigne au cours de l'analyse, dans l'onglet **Info**, ouvrez le menu **Paramètres** et définissez le paramètre **Rétro-éclairage** à **Actif**. Par défaut, après un moment sans appuyer sur les touches du smartphone, le rétro-éclairage s'éteint afin d'économiser les batteries.

2.2.6.2. Planification de l'analyse

Kaspersky Anti-virus permet de planifier des analyses automatiques, qui seront lancés à une heure spécifique. L'analyse sera effectuée en arrière-plan. En cas de détection d'un objet infecté, l'application exécute l'action spécifiée par les paramètres d'analyse (voir section 2.2.4 à la page 15).

L'analyse programmée est désactivée par défaut.

Pour configurer une analyse planifiée, procédez de la manière suivante :

Utilisez la page **Analyser** pour sélectionner **Planification** et configurez les paramètres **Analyse auto** (voir fig. 15) :

- **Quotidien** – le smartphone sera analysé tous les jours. Dans le champ en dessous, spécifiez l'**Heure d'analyse auto.**.

- **Hebdomadaire** – le smartphone sera analysé toutes les semaines. Dans le champ en dessous, spécifiez le **Jour d'analyse auto.** et l'**Heure d'analyse auto.**.

Figure 15. Le menu **Planification**

2.2.7. Utilisation de la quarantaine

La quarantaine est l'une de nouvelles caractéristiques introduites par Kaspersky Anti-virus® Mobile 6.0 après la version 1.7. Les objets infectés placés en quarantaine ne sont pas en mesure d'endommager votre smartphone et peuvent être supprimés ou restaurés par la suite.

Le logiciel peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Si vous souhaitez configurer l'application pour placer automatiquement en quarantaine les objets infectés, ouvrez la page **Analyser**, sélectionnez **Paramètres** puis choisissez la valeur **Quarantaine** pour le paramètre **Action anti-virus**.

Si vous avez choisi l'action **Demander**, lors de la détection d'un objet infecté, Kaspersky Anti-virus vous proposera son effacement ou son déplacement en quarantaine.

La page **Quarantaine** permet de consulter les caractéristiques principales de la quarantaine (voir fig. 16).

Figure 16. Le menu **Quarantaine**

Sélectionnez **Quarantaine** pour afficher la liste de tous les objets en quarantaine (voir fig. 17).

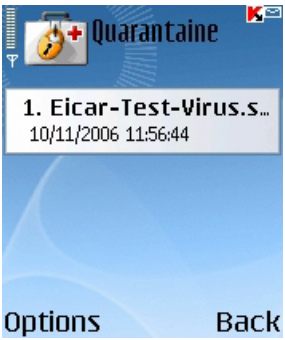

Figure 17. Objets infectés en quarantaine

Le menu **Options** dans cette fenêtre vous permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Détails**).
- Supprimer l'objet courant (**Supprimer fichier**).
- Purger la quarantaine en supprimant tous les objets conservés (**Tout supprimer**).
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer fichier**).

- Afficher de l'aide sur le fonctionnement de la quarantaine (**Aide**).

Pour configurer la quarantaine, utilisez le menu **Paramètres** de la page **Quarantaine** (voir fig. 18).

Figure 18. Paramètres de quarantaine

Le paramètre **Taille de la quarantaine** définit le nombre maximum d'objets infectés pouvant être conservés en quarantaine. Vous pouvez spécifier une valeur de **20**, **50** ou **100** fichiers.

Le paramètre **Conservation** définit la période pendant laquelle les objets infectés peuvent rester en quarantaine. Le logiciel supprimera automatiquement les objets infectés à la fin de la période spécifiée.

Si vous souhaitez restaurer la configuration de quarantaine recommandée par les experts de Kaspersky Lab, sélectionnez **Par défaut** dans le menu **Options**.

2.2.8. Utilisation du composant Anti-Spam

Le composant Anti-Spam est un autre caractéristique nouvelle introduite par Kaspersky Anti-virus Mobile 6.0. Il est destiné à protéger le smartphone contre les messages SMS et MMS indésirables.

Le principe utilisé pour filtrer les messages fait appel aux listes dites noire et blanche. Le composant Anti-Spam permet de bloquer les messages entrants provenant de numéros de téléphone ajoutés à votre liste noire. Les messages provenant de numéros ajoutés à la liste blanche ne seront pas bloqués. Tout en créant ces listes, vous pouvez également spécifier le type des messages (SMS ou MMS) qui seront bloqués ou autorisés.

2.2.8.1. Modes du composant Anti-Spam

Pour configurer le composant Anti-Spam, ouvrez l'onglet **Info** et sélectionnez **Paramètres généraux**. Définissez l'un des modes suivants du paramètre **Anti-Spam** :

- **Activer**. Dans ce mode, le composant Anti-Spam filtre les messages entrants à partir des listes noire et blanche. Quand un message est envoyé par un numéro qui ne figure dans aucune de ces listes, le composant Anti-Spam affiche un message proposant de bloquer ou d'autoriser la réception du message et d'ajouter le numéro de téléphone à la liste blanche ou noire.

- **Listes B/N uniquement**. Dans ce mode, le composant Anti-Spam filtre les messages entrants à partir des listes noire et blanche uniquement. La réception de messages de numéros de téléphone qui ne sont pas inclus dans l'une des listes est autorisée, sans demander confirmation à l'utilisateur.

- **Désactiver**. Le composant antipourriel est désactivé dans ce mode. Les messages entrants ne seront pas filtrés.

2.2.8.2. Modification des listes noire et blanche

La liste « noire » contient des numéros de téléphone dont la réception de messages SMS ou MMS est bloquée par le composant Anti-Spam.

La liste « blanche » contient des numéros de téléphone dont la réception de messages SMS ou MMS est autorisée.

Les messages provenant de numéros qui ne figurent dans aucune des listes ne seront pas bloqués !

Pour pouvoir modifier votre liste noire ou blanche, ouvrez la page **Anti-Spam** (voir fig. 19) et sélectionnez la liste souhaitée.

Figure 19. Le menu **Anti-Spam**

Utilisez le menu **Options** pour modifier la liste :

- **Ajouter enregistrement –** ajoute un nouvel enregistrement à la liste sélectionnée.
- **Modifier enregistrement –** modifie l'enregistrement sélectionné.
- **Supprimer enregistrement –** supprime l'enregistrement courant de la liste.
- **Tout supprimer –** réinitialise la liste en supprimant tous les enregistrements.

Si vous sélectionnez **Ajouter enregistrement** ou **Modifier enregistrement**, vous devez spécifier les paramètres suivants de l'enregistrement :

- **Type de message**. Spécifie le type des messages entrants qui seront bloqués ou autorisés (d'après la liste noire ou blanche, respectivement). Valeurs possibles : **SMS seuls**, **MMS seuls** ou **Tous messages**.
- **Indiquez le téléphone**. Spécifie le numéro de téléphone d'où proviennent les messages à bloquer ou à autoriser. Le numéro peut commencer par un chiffre ou par le signe "+" ; il ne peut contenir que des chiffres.

Une fois indiquées les valeurs des paramètres précédents, appuyez sur **Précédent** pour enregistrer les modifications et revenir à la fenêtre de liste (voir fig. 20).

Figure 20. Liste noire

2.2.8.3. Paramètres antipourriel

Pour configurer le composant Anti-Spam, ouvrez l'onglet **Anti-Spam** et sélectionnez **Paramètres** (voir fig. 21).

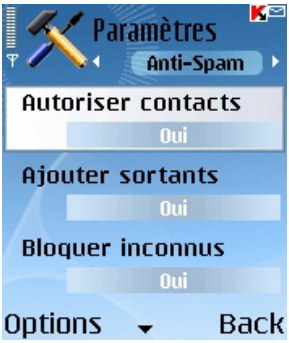

Figure 21. Paramètres antipourriel

Dans le menu paramètres, vous pouvez personnaliser les paramètres antipourriel suivants :

- **Autoriser contacts**. Si le paramètre est défini à **Oui**, le composant Anti-Spam ne bloquera pas la réception de messages provenant de numéros de téléphone inclus dans votre répertoire. Si l'option est désactivée (le paramètre est défini à **Non**), le composant Anti-Spam vérifiera les messages en contrôlant l'expéditeur dans la liste blanche ou noire.

- **Ajouter sortants**. Si le paramètre est défini à **Oui**, le composant Anti-Spam ajoutera automatiquement à la liste blanche tous les numéros de téléphone utilisés pour envoyer des messages SMS ou MMS. Sélectionnez **Non** pour désactiver l'option.

- **Bloquer inconnus**. Si le paramètre est défini à **Non**, le composant Anti-Spam ne bloquera pas les messages entrants provenant de numéros de téléphone masqués. Choisissez **Oui** pour activer l'option.

- **Distinguer msg par type**. Si le paramètre a la valeur **Non**, la valeur **Tous messages** sera utilisée pour le type des messages des nouveaux enregistrements de la liste blanche ou noire (reportez-vous à la section 2.2.8.2 à la page 25 pour plus de détails sur les paramètres des enregistrements des listes) autrement, les nouveaux enregistrements seront créés selon le type de message spécifique (SMS ou MMS).

Ce paramètre affectera les enregistrements créés par le composant Anti-Spam uniquement dans les cas suivants :

- L'ajout de numéros sortants à la liste blanche (l'option **Ajouter sortants** est activée).

- L'ajout des numéros de téléphone d'où proviennent les nouveaux messages, à l'une des listes (voir section 2.2.8.4 à la page 28 pour plus de détails).

- Pour modifier les valeurs des paramètres, utilisez le joystick de votre smartphone ou sélectionnez **Modifier** dans le menu **Options**.

2.2.8.4. Actions appliquées aux messages

Quand vous recevez un message SMS ou MMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, le composant Anti-Spam intercepte le message et affiche le message correspondant (voir fig. 22).

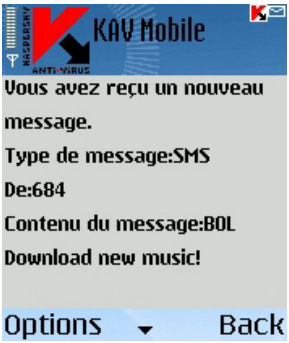

Figure 22. Message du composant Anti-Spam

Vous pouvez utiliser le menu **Options** pour sélectionner et appliquer l'une des actions suivantes au message :

- **Ajouter à la liste blanche** – autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.
- **Ajouter à la liste noire** – bloque la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.
- **Ignorer le message** – autorise la réception du message. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Si le paramètre **Distinguer msg. par type** de la configuration antipourriel est définit à **Non**, alors les actions **Ajouter à la liste blanche** ou **Ajouter à la liste noire** créeront respectivement un enregistrement pour tous les messages dans la liste correspondante (**Type de message** – **Tous messages**), autrement le type correspondra au type du message reçu. Reportez-vous à la section 2.2.8.2 à la page 25 pour plus de détails sur les paramètres des enregistrements de liste.

Des informations sur les messages bloqués sont ajoutées au rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Info** et sélectionnez **Rapports**.

2.2.9. Mise à jour des bases anti-virus

Kaspersky Anti-virus détecte les virus grâce aux enregistrements de ses bases anti-virus qui contiennent la description de tous les logiciels nocifs connus. Il est

extrêmement important de protéger la sécurité de votre smartphone en mettant à jour fréquemment les bases anti-virus.

Vous pouvez lancer la mise à jour manuellement ou programmer son exécuter automatique à une heure spécifiée. Les mises à jour peuvent être téléchargées depuis les serveurs de mise à jour de Kaspersky Lab ou à partir d'un dossier local (voir section 2.2.9.1 à la page 30 à propos des méthodes de mise à jour).

Vous pouvez configurer l'application pour analyser automatiquement le système de fichiers du smartphone après chaque mise à jour. Pour ce faire, ouvrez la page **Mise à jour**, sélectionnez **Paramètres** et définissez l'option **Analyser après la mise à jour** à **Actif**.

Le paramètre **Analyser Quar. après mise à jour** permet d'activer ou désactiver l'analyse des objets en quarantaine après chaque mise à jour des bases anti-virus. L'analyse est activée par défaut. Pour la désactiver, sélectionnez **Inactif**.

Si vous ne souhaitez pas sélectionner un point d'accès lors de chaque mise à jour, donnez au paramètre **Demander le point d'accès** la valeur **Inactif**. Le programme mémorisera alors le dernier point d'accès utilisé avec succès et effectuera les mises à jour suivantes en se connectant au même point.

Le paramètre **Serveur de mise à jour** définit la source des mises à jour de la bases anti-virus : serveurs de mise à jour de Kaspersky Lab ou serveur spécifié par l'utilisateur. Si le paramètre est défini à **personnalisé**, la liste des options s'élargit pour en inclure une autre, le **nom de l'URL**. Vous pouvez spécifier un serveur alternatif, si nécessaire.

Pour afficher les informations sur la base de données en cours, ouvrez l'onglet **Info** et sélectionnez **Info base de données**.

Les informations de mise à jour sont enregistrées dans le rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Info** et sélectionnez **Rapports**.

2.2.9.1. Sélectionnez la méthode de mise à jour

Pour sélectionner l'origine des mises à jour, procédez de la manière suivante:

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).

2. Dans la page **Mise à jour** sélectionnez **Paramètres** (voir fig. 23).

Figure 23. La page **Mise à jour**

3. Sélectionnez la source de la mise à jour :

   - Mises à jour locales : l'application utilisera les mises à jour des bases disponibles dans votre smartphone. Pour sélectionner ce type de mise à jour, définissez la valeur à **Chercher dans le téléphone**.

   - Mises à jour Web : l'application téléchargera les mises à jour à partir des serveurs de Kaspersky Lab. Pour sélectionner ce mode de mise à jour, définissez la valeur à **Mise à jour WAP**, pour utiliser WAP, ou à **Mise à jour HTTP** pour télécharger les mises à jour en utilisant le protocole HTTP. Sélectionnez **Avec navigateur** pour recevoir les mises à jour à l'aide du navigateur de votre smartphone.

Pour mettre à jour la base depuis Internet, votre smartphone doit disposer d'une connexion GPRS (pour la mise à jour via HTTP) ou une connexion WAP.

Si Kaspersky Anti-virus est configuré pour faire la mise à jour à partir d'un fichier local, copiez le fichier de la nouvelle base dans le smartphone par n'importe lequel des moyens habituels. Quand la mise à jour démarre, Kaspersky Anti-virus détecte automatiquement le fichier avec les bases les plus récentes et remplace l'ancien fichier par le nouveau.

Si vous sélectionnez la mise à jour en utilisant un navigateur Web, au démarrage de Kaspersky Anti-virus, celui-ci lancera le navigateur Web du smartphone, téléchargera les mises à jour et les recopiera automatiquement dans le répertoire de travail.

Si Kaspersky Anti-virus est configuré pour faire la mise à jour par Internet :

1. Activer / Désactiver la demande de point d'accès (paramètre Demander le point d'accès).

   Vous pouvez définir un point d'accès à partir des informations fournies par votre opérateur.

   Si vous sélectionnez **Inactif**, la connexion se réalisera en utilisant le dernier point d'accès utilisé pour la mise à jour.

   Si la demande est active, vous aurez à faire le choix dans une liste de point d'accès disponibles (voir fig. 24).

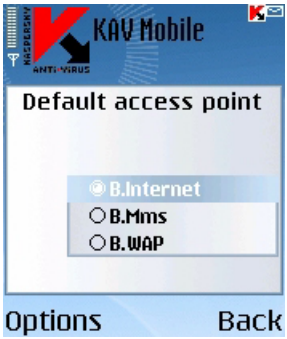

Figure 24. Sélection d'un point d'accès

2. Si nécessaire, utilisez la commande Url de mise à jour pour spécifier l'adresse du serveur de mise à jour.

Figure 25. URL du serveur de mise à jour

Par défaut, les mises à jour sont récupérées d'un serveur de Kaspersky Lab à l'adresse : http://ftp.kaspersky.com/index/mobile.xml.

La mise à jour sera suivie par la déconnexion Internet, même si la connexion était déjà établie.

2.2.9.2. Mise à jour manuelle

Pour lancer la mise à jour des bases anti-virus manuellement:

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).
2. Sélectionnez la source de la mise à jour (voir section 2.2.9.1 à la page 30).
3. Dans l'onglet Mise à jour sélectionnez Mise à jour (voir fig. 23).

2.2.9.3. Mise à jour programmée

Pour planifier les mises à jour des base anti-virus,

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).
2. Sélectionnez la source de la mise à jour (voir section 2.2.9.1 à la page 30).
3. Utilisez la page Mise à jour pour sélectionner Planification et configurez les paramètres de Mise à jour automatique :
    - **Quotidien** – exécute la mise à jour une fois par jour. Spécifiez l'**Heure de mise à jour automatique**.
    - **Hebdomadaire** – exécute la mise à jour une fois par semaine. Spécifiez le **Jour de mise à jour automatique** et l'**Heure de mise à jour automatique**.

2.2.10. Renouvellement de la licence

Pour rallonger la durée de votre licence d'utilisation du programme, procédez comme ceci:

1. Lancez Kaspersky Anti-virus (voir section 2.2.2 à la page 13).

2. Ouvrez le menu **Info**, sélectionnez **Licence** puis Renouveler.

3. Suivez les instructions de la section 2.2.1 à la page 12 pour saisir le nouveau code dans la fenêtre d'activation.

Vous pouvez également afficher des informations associées à la clé courante ainsi que sa période de validité avec la commande Informations du menu Licence KAV (voir fig. 26).

Figure 26. Gestion des licences

2.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus de votre smartphone :

1. Quittez le programme. Pour ce faire :

   - Maintenez appuyé le bouton **Menu**.
   - Sélectionnez **KAV Mobile** dans la listes des applications en exécution. Cliquez ensuite sur **Options**.
   - Sélectionnez la commande **Quitter** (voir fig. 27).

Figure 27. Sortie du logiciel

2. Supprimez Kaspersky Anti-Virus :

   - Appuyez sur **Menu** puis sélectionnez **Gestionnaire d'applications**. (voir fig. 28).

Figure 28. **Gestionnaire d'applications** – démarrage

   - Sélectionnez **KAV Mobile** dans la listes des applications en exécution. Cliquez ensuite sur **Options** (voir fig. 29).

Figure 29. Sélection du programme

- Sélectionnez la commande **Supprimer** (voir fig. 30).

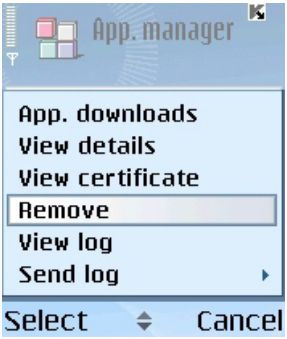

Figure 30. Suppression du programme

- Pour confirmer la suppression du programme, appuyez sur **Oui** (voir fig. 31).

Figure 31. Confirmation de la suppression du programme

CHAPITRE 3. KASPERSKY ANTI-VIRUS FOR SYMBIAN UIQ OS

Ce chapitre décrit le fonctionnement de Kaspersky Anti-virus Mobile sur des smartphones sous système d'exploitation Symbian Series UIQ. La version de l'application conçue pour des smartphones exploités sous les systèmes d'exploitation Symbian 6.1, 7.0s, 8.0 ou Series 60 UI est décrite en détail dans Chapitre 2.

3.1. Installation de Kaspersky Anti-virus

Pour installer Kaspersky Anti-virus Mobile, procédez de la manière suivante:

3. Copiez le paquet d'installation de l'application dans votre smartphone.

4. Exécutez l'installation (ouvrez le fichier de distribution dans votre smartphone).

5. Si un avertissement de protection est affiché, choisissez **Oui** (voir fig. 32)[2].

[2] Toutes les illustrations de ce document ont été capturées sur un smartphone modèle Nokia 6670. Sur d'autres modèles de smartphones, l'interface de l'application peut varier.

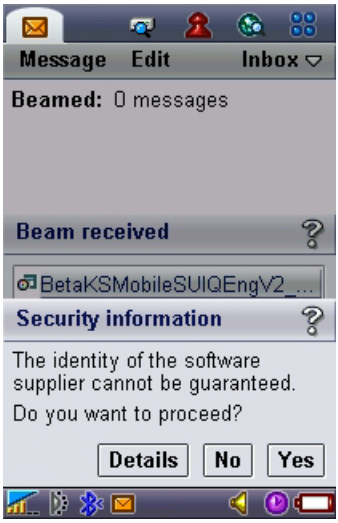

Figure 32. Avertissement de protection

6. Pour confirmer l'installation, choisissez **Oui** (voir fig. 33).

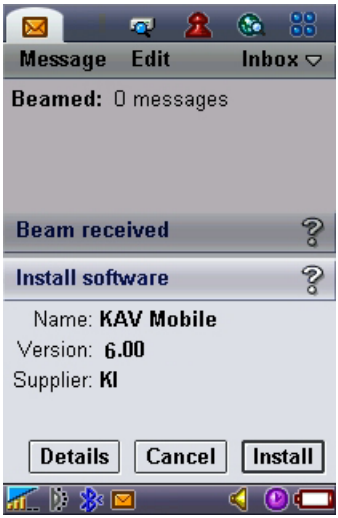

Figure 33. Confirmation de l'installation

7. Sélectionnez l'emplacement d'installation de l'application : dans la mémoire du smartphone ou sur une carte d'extension (voir fig. 34).

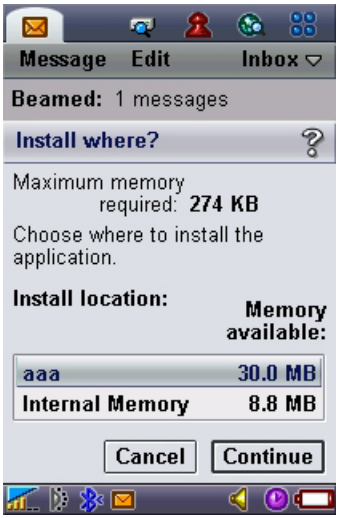

Figure 34. Sélectionnez l'emplacement d'installation de l'application

8. Lisez le contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **Oui**. Pour abandonner l'installation, appuyez sur **Annuler** (voir fig. 35).

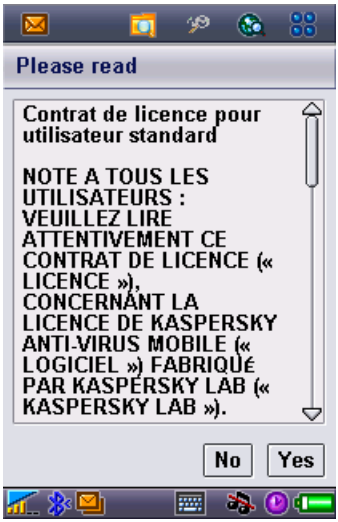

Figure 35. Contrat de licence

3.2. Utilisation de l'application

Cette section décrit la configuration de l'anti-virus et de la protection en temps réel, le filtrage des messages SMS et MMS, l'analyse anti-virus du terminal et les mises à jour de l'application.

3.2.1. Activation du logiciel

Lors de son premier démarrage, le logiciel affiche une boîte de dialogue proposant d'activer Kaspersky Anti-virus (voir fig. 36).

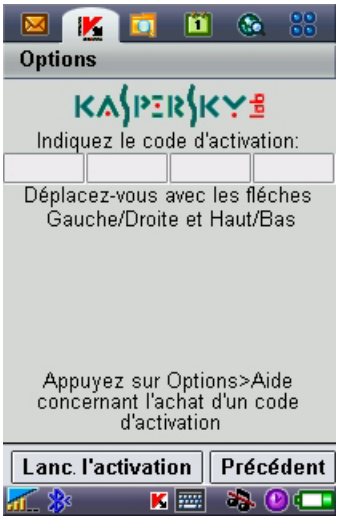

Figure 36. Boîte de dialogue d'activation du programme

L'activation du programme est nécessaire pour autoriser toutes les fonctionnalités de Kaspersky Anti-virus. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab.

Attention !

Une connexion GPRS est nécessaire pour activer Kaspersky Anti-virus Mobile 6.0 sur un smartphone.

Le code d'activation est composé de lettres et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus. Utilisez les boutons « Haut/Bas » pour vous déplacer aux champs précédent ou suivant.

Après avoir saisi le code d'activation, choisissez la commande **Lancer l'activation** dans le menu **Options**. L'application enverra une pétition HTTP à un serveur d'activation de Kaspersky Lab puis elle téléchargera et installera une clé de licence.

Si le code d'activation saisi s'avère être incorrect pour une raison ou une autre, le programme affiche un message correspondant.

3.2.2. Lancement de l'application

Pour lancer Kaspersky Anti-virus Mobile, procédez de la manière suivante:

1. Ouvrez la liste des applications installées dans le smartphone.

2. Sélectionnez l'icône  KAV Mobile et lancez l'application avec l'option **Ouvrir** dans le menu **Options**.

Après le démarrage de l'application, le smartphone affiche une fenêtre décrivant l'état des composants principaux de Kaspersky Anti-virus (voir fig. 37).

- **Protection en temps réel** – état de la protection en temps réel. Pour plus de détails, voir section 3.2.5 à la page 47.

- **Dernière analyse complète** – date et heure de la dernière analyse anti-virus du smartphone.

- **Date de la base de données** – date de publication de la base utilisée par l'application.

- **Config. Anti-Spam** – Mode de fonctionnement du composant Anti-Spam. Pour plus de détails sur les modes d'exploitation, voir section 3.2.8.1 à la page 57.

Figure 37. Fenêtre d'état des composants de l'application

Pour revenir à l'interface de l'application, cliquez sur .

3.2.3. Interface graphique utilisateur

L'interface graphique contient présente onglets :

L'onglet **Analyse** permet d'effectuer une analyse anti-virus du smartphone, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique.

L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.

L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de modifier les paramètres et de planifier la mise à jour.

L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS et MMS entrants.

L'onglet **Info** permet d'afficher les rapports d'activité des composants de l'application, des informations générales sur l'application et la base anti-virus utilisée, ainsi que de modifier les paramètres généraux de l'application.

Pour vous déplacer d'un onglet à l'autre, utilisez le joystick de votre smartphone ou sélectionnez l'entrée correspondante du menu **Options** (voir fig. 38).

Figure 38. Le menu **Options**

Pour revenir à la fenêtre d'état des composants de l'application, sélectionnez **État actuel** dans le menu **Options**.

3.2.4. Paramètres généraux

Les paramètres de l'onglet **Info** dans la page **Paramètres** (voir fig. 39) permettent de configurer les caractéristiques suivantes de l'application :

- Le mode d'exploitation du composant Anti-Spam (**Configurer Anti-Spam**). Sélectionnez **Activer** pour activer toutes les fonctions du composant Anti-Spam. Choisissez **Listes B/N uniquement** pour que le composant Anti-Spam utilise uniquement les listes noire et blanche. Sélectionnez **Désactiver** pour désactiver le composant Anti-Spam (reportez-vous à la section 3.2.8 à la page 56 pour plus de détails sur l'usage du composant Anti-Spam).

- Ajout du programme au dossier Favoris (**Ajouter aux Favoris**). Choisissez **Oui** pour ajouter un raccourci vers l'application dans le dossier Favoris.

- Une option pour afficher l'état courant à chaque démarrage du programme (**Voir écran d'état**).

- Le nombre d'enregistrements conservés dans le rapport de l'application (**Taille rapport**).

- L'utilisation du rétro-éclairage pendant l'analyse du système de fichiers à la recherche de virus (**Rétro-éclairage**).

- L'utilisation de sons (**Activer le son**) pour communiquer certains événements (détection d'un objet infecté, informations sur l'état du programme, etc.). Sélectionnez **Actif** si vous souhaitez entendre des notifications sonores.

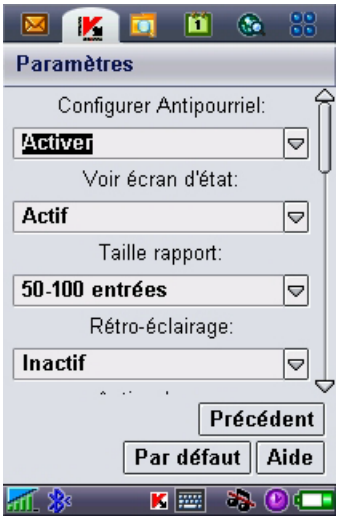

Figure 39. Le menu **Paramètres**

Pour modifier les valeurs des paramètres, utilisez le joystick de votre smartphone ou sélectionnez **Modifier** dans le menu **Options**.

3.2.5. Protection en temps réel des fichiers

Dans le mode de protection en temps réel, la partie résidente de Kaspersky Anti-virus reste en permanence dans la mémoire de votre smartphone, pour surveiller toutes les données ou seulement les données entrantes (en fonction des paramètres sélectionnés).

Le mode de protection en temps réel reste activé depuis le démarrage jusqu'à l'arrêt du smartphone (à moins que ce mode ne soit désactivé par configuration).

Les résultats de l'analyse sont enregistrés dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Info**.

Pour modifier la configuration de la protection en temps réel:

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).

2. Sur l'onglet **Analyse**, sélectionnez **Paramètres** (voir fig. 40).

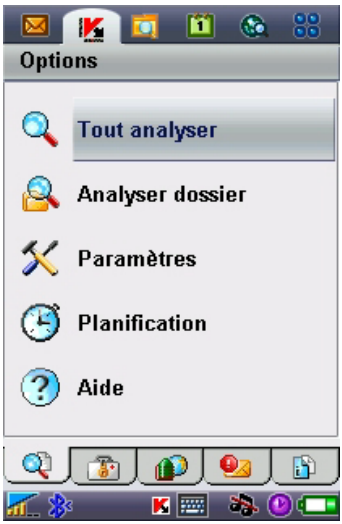

Figure 40. Onglet **Analyse**

3. Dans le menu ouvert à la suite, configurez les paramètres nécessaires (voir fig. 41) :

Figure 41. Le menu **Paramètres**

- Activer / Désactiver la protection en temps réel (paramètre **Protection en temps réel**).

  Par défaut, dans le mode de protection en temps réel, l'application analyse toutes les données entrantes (l'option **Entrants seuls** est sélectionnée).

  Pour configurer Kaspersky Anti-virus afin d'analyser tous les fichiers entrants et le système de fichiers complet, sélectionnez **Tout analyser**.

  Pour désactiver la protection en temps réel, sélectionnez **Inactif**.

- Sélectionnez les types de fichiers à analyser (option **Masque**) :

  - **Tous les fichiers** – analyse les fichiers de tous formats.

  - **Fichiers exécutables** – analyse uniquement les fichiers exécutables (par exemple, les fichiers avec extensions *.exe, *.sis, *.mdl ou *.app).

- Définissez l'action à réaliser en cas de détection d'un objet infecté (paramètre **Action anti-virus**).

  Si vous souhaitez afficher une confirmation avant d'appliquer l'action spécifiée, sélectionnez **Demander**.

  Si vous souhaitez que Kaspersky Anti-virus supprime automatiquement les messages infectés sans demander la confirmation de l'utilisateur, choisissez **Suppression auto**.

  Sélectionnez **Quarantaine** pour déplacer les objets détectés vers la quarantaine.

- Activer / Désactiver l'analyse de la mémoire ROM des smartphone (paramètre **Analyser ROM**).

  En certains cas, la mémoire ROM peut être vulnérable aux applications malveillantes. Pour configurer Kaspersky Anti-virus afin d'analyser cette mémoire, sélectionnez **Oui**.

  Pour désactiver l'analyse de la ROM, sélectionnez **Non**.

- Activer / Désactiver la décompression des archives SIS (paramètre **Décompresser archives**). Sélectionnez **Oui** afin que Kaspersky Anti-virus décompresse les archives SIS lors de l'analyse. Si vous n'avez pas besoin de décompresser les archives SIS au cours de l'analyse, désactivez cette caractéristique avec **Non**.

- Activer / Désactiver l'analyse des nouvelles cartes mémoire (paramètre **Analyser carte**). Pour que Kaspersky Anti-virus analyse automatiquement les cartes de mémoire flash connectées à votre smartphone, sélectionnez **Analyse auto.** Sélectionnez **Désactiver** pour annuler l'analyse automatique des cartes de mémoire flash. Pour faire en sorte que Kaspersky Anti-virus Mobile propose d'analyser chaque nouvelle carte insérée, sélectionnez **Demander**.

- Afficher / Masque l'icône de protection en temps réel (paramètre **Afficher l'icône PTR**).

  Pour que l'application affiche l'icône chaque fois que protection en temps réel est activée, sélectionnez **Toujours**. Si vous souhaitez afficher l'icône uniquement dans le menu du

smartphone, sélectionnez **Menu uniquement**. Pour masquer l'icône, sélectionnez **Jamais**.

3.2.6. Analyse à la demande

Dans le mode d'*analyse à la demande*, l'application analyse votre smartphone à la recherche de logiciels nocifs à la demande de l'utilisateur ou à une heure programmée d'avance.

Kaspersky Anti-virus peut réaliser une analyse complète du système de fichiers de votre smartphone, y compris les objets conservés sur les cartes d'extension mémoire.

Les résultats de l'analyse sont enregistrés dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Info**.

La configuration de la protection en temps réel, décrite dans la section 3.2.5 à la page 47 s'applique également à l'analyse à la demande. En outre, les analyses à la demande utilisent des paramètres supplémentaires qui sont décrits plus en détail dans la suite.

3.2.6.1. Exécution manuelle d'une analyse

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

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).

2. Utilisez l'onglet **Analyse** (voir fig. 40) pour sélectionner **Tout analyser**, si vous souhaitez contrôler le système de fichiers complet de votre smartphone, ou **Analyser dossier** pour analyser le contenu d'un dossier individuel.

   La sélection de la commande **Analyser dossier** présente une fenêtre avec le système de fichiers du smartphone. Utilisez les boutons du joystick pour vous déplacer dans le système de fichiers. Pour lancer l'analyse d'un dossier, placez le curseur sur ce dernier puis sélectionnez **Analyser** dans le menu **Options**.

Dès que la procédure démarre, une fenêtre affiche la progression de l'analyse, avec les indicateurs en cours : nombre d'objets analysés, chemin vers l'objet en

cours d'analyse et une barre progression avec le pourcentage d'objets analysés (voir fig. 42).

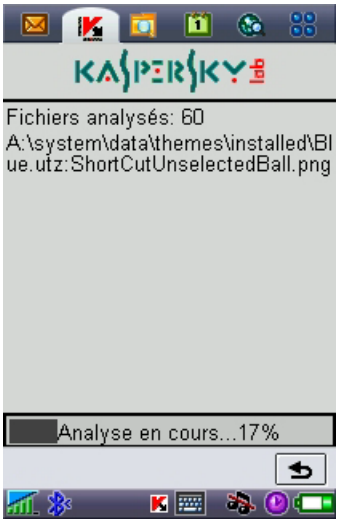

Figure 42. Écran de progression de l'analyse

En cas de détection d'un objet infecté, l'application propose de supprimer le fichier concerné (action **Supprimer**), de le placer en quarantaine (action **Déplacer vers quarantaine**) ou de laisser tel quel le fichier (action **Ignorer**).

Le logiciel n'affichera le choix des action possible que si le paramètre **Action anti-virus** a été définit à **Demander** (voir section 3.2.5 à la page 47 pour plus de détails).

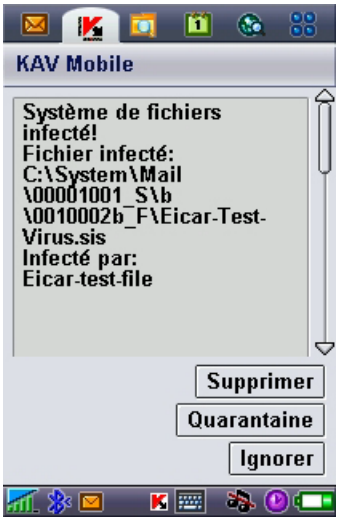

Figure 43. Notification de détection de virus

Après l'analyse, des statistiques globales sur le objets infectés /supprimés sont affichées.

Pour éviter que le rétro-éclairage ne s'éteigne au cours de l'analyse, dans l'onglet **Info**, ouvrez le menu **Paramètres généraux** et définissez le paramètre **Rétro-éclairage** à **Actif**. Par défaut, après un moment sans appuyer sur les touches du smartphone, le rétro-éclairage s'éteint afin d'économiser les batteries.

3.2.6.2. Planification de l'analyse

Kaspersky Anti-virus permet de planifier des analyses automatiques, qui seront lancés à une heure spécifique. L'analyse sera effectuée en arrière-plan. En cas de détection d'un objet infecté, l'application exécute l'action spécifiée par les paramètres d'analyse (voir section 3.2.4 à la page 45).

L'analyse programmée est désactivée par défaut.

Pour configurer une analyse planifiée, procédez de la manière suivante :

Utilisez la page **Analyser** pour sélectionner **Planification** et configurez les paramètres **Analyse auto** (voir fig. 44) :

- **Quotidien** – le smartphone sera analysé tous les jours. Dans le champ en dessous, spécifiez l'**Heure d'analyse auto.**.

- **Hebdomadaire** – le smartphone sera analysé toutes les semaines. Dans le champ en dessous, spécifiez le **Jour d'analyse auto.** et l'**Heure d'analyse auto.**.

Figure 44. Le menu **Planification**

3.2.7. Utilisation de la quarantaine

La quarantaine est l'une de nouvelles caractéristiques introduites par Kaspersky Anti-virus® Mobile 6.0 après la version 1.7. Les objets infectés placés en quarantaine ne sont pas en mesure d'endommager votre smartphone et peuvent être supprimés ou restaurés par la suite.

Le logiciel peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Si vous souhaitez configurer l'application pour placer automatiquement en quarantaine les objets infectés, ouvrez la page **Analyser**, sélectionnez **Paramètres** puis choisissez la valeur **Quarantaine** pour le paramètre **Action anti-virus**.

Si vous avez choisi l'action **Demander**, lors de la détection d'un objet infecté, Kaspersky Anti-virus vous proposera son effacement ou son déplacement en quarantaine.

La page **Quarantaine** permet de consulter les caractéristiques principales de la quarantaine (voir fig. 45).

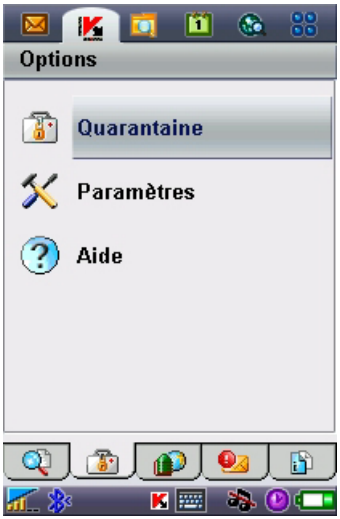

Figure 45. Le menu **Quarantaine**

Sélectionnez **Quarantaine** pour afficher la liste de tous les objets en quarantaine (voir fig. 46).

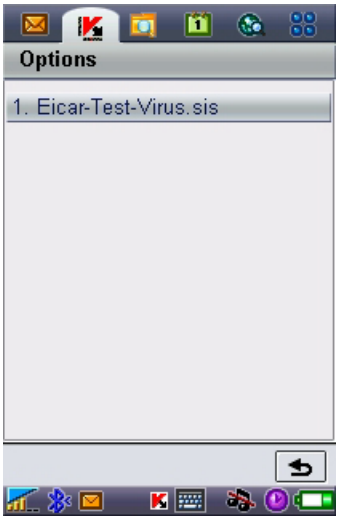

Figure 46. Objets infectés en quarantaine

Le menu **Options** dans cette fenêtre vous permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Détails**).
- Supprimer l'objet courant (**Supprimer fichier**).
- Purger la quarantaine en supprimant tous les objets conservés (**Tout supprimer**).
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer fichier**).
- Afficher de l'aide sur le fonctionnement de la quarantaine (**Aide**).

Si vous souhaitez configurer la quarantaine, utilisez le menu **Paramètres de quarantaine** de la page **Quarantaine** (voir fig. 47).

Figure 47. Paramètres de quarantaine

Le paramètre **Taille de la quarantaine** définit le nombre maximum d'objets infectés pouvant être conservés en quarantaine. Vous pouvez spécifier une valeur de **20**, **50** ou **100** fichiers.

Le paramètre **Conservation** définit la période pendant laquelle les objets infectés peuvent rester en quarantaine. Le logiciel supprimera automatiquement les objets infectés à la fin de la période spécifiée.

Si vous souhaitez restaurer la configuration de quarantaine recommandée par les experts de Kaspersky Lab, sélectionnez **Par défaut** dans le menu **Options**.

3.2.8. Utilisation du composant Anti-Spam

Le composant Anti-Spam est un autre caractéristique nouvelle introduite par Kaspersky Anti-virus Mobile 6.0. Il est destiné à protéger le smartphone contre les messages SMS et MMS indésirables.

Le principe utilisé pour filtrer les messages fait appel aux listes dites noire et blanche. Le composant Anti-Spam permet de bloquer les messages entrants provenant de numéros de téléphone ajoutés à votre liste noire. Les messages provenant de numéros ajoutés à la liste blanche ne seront pas bloqués. Tout en

créant ces listes, vous pouvez également spécifier le type des messages (SMS ou MMS) qui seront bloqués ou autorisés.

3.2.8.1. Modes du composant Anti-Spam

Pour configurer le composant Anti-Spam, ouvrez l'onglet **Info** et sélectionnez **Paramètres généraux**. Définissez l'un des modes suivants à l'aide du paramètre **Anti-Spam** :

- **Activer**. Dans ce mode, le composant Anti-Spam filtre les messages entrants à partir des listes noire et blanche. Quand un message est envoyé par un numéro qui ne figure dans aucune de ces listes, le composant Anti-Spam affiche un message proposant de bloquer ou d'autoriser la réception du message et d'ajouter le numéro de téléphone à la liste blanche ou noire.

- **Listes noire/blanche uniquement**. Dans ce mode, le composant Anti-Spam filtre les messages entrants à partir des listes noire et blanche uniquement. La réception de messages de numéros de téléphone qui ne sont pas inclus dans l'une des listes est autorisée, sans demander confirmation à l'utilisateur.

- **Désactiver**. Le composant antipourriel est désactivé dans ce mode. Les messages entrants ne seront pas filtrés.

3.2.8.2. Modification des listes noire et blanche

Le composant Anti-Spam utilise des listes « noire » et « blanche » pour identifier les numéros de téléphone des messages entrants, respectivement pour les bloquer ou les autoriser.

Pour pouvoir modifier votre liste noire ou blanche, ouvrez la page **Anti-Spam** (voir fig. 48) et sélectionnez la liste souhaitée.

Figure 48. Le menu **Anti-Spam**

Utilisez le menu **Options** pour modifier la liste :

- **Ajouter enregistrement** – ajoute un nouvel enregistrement à la liste sélectionnée.
- **Modifier enregistrement** – modifie l'enregistrement sélectionné.
- **Supprimer enregistrement** – supprime l'enregistrement courant de la liste.
- **Tout supprimer** – réinitialise la liste en supprimant tous les enregistrements.

Si vous sélectionnez **Ajouter enregistrement** ou **Modifier enregistrement**, vous devez spécifier les paramètres suivants de l'enregistrement :

- **Type de message**. Spécifie le type des messages entrants qui seront bloqués ou autorisés (d'après la liste noire ou blanche, respectivement). Valeurs possibles : **SMS seuls**, **MMS seuls** ou **Tous messages**.
- **Indiquez le téléphone**. Spécifie le numéro de téléphone d'où proviennent les messages à bloquer ou à autoriser. Le numéro peut commencer par un chiffre ou par le signe "+" ; il ne peut contenir que des chiffres.

Une fois indiquées les valeurs des paramètres précédents, appuyez sur **OK** pour enregistrer les modifications et revenir à la fenêtre de liste (voir fig. 49).

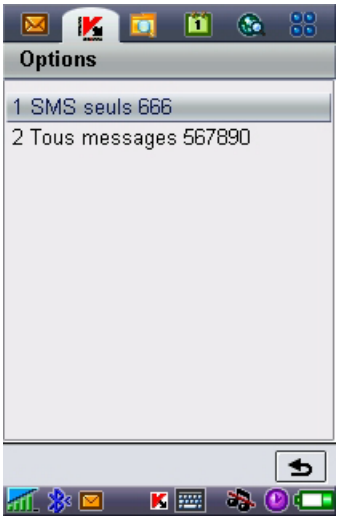

Figure 49. Liste noire

3.2.8.3. Paramètres antipourriel

Pour configurer le composant Anti-Spam, ouvrez l'onglet **Anti-Spam** et sélectionnez **Paramètres antipourriel** (voir fig. 50).

Figure 50. Paramètres antipourriel

Dans le menu paramètres, vous pouvez personnaliser les paramètres antipourriel suivants :

- **Autoriser contacts**. Si le paramètre est défini à **Oui**, le composant Anti-Spam ne bloquera pas la réception de messages provenant de numéros de téléphone inclus dans votre répertoire. Si l'option est désactivée (le paramètre est défini à **Non**), le composant Anti-Spam vérifiera les messages en contrôlant l'expéditeur dans la liste blanche ou noire.

- **Autoriser les messages sortants**. Si le paramètre est défini à **Oui**, le composant Anti-Spam ajoutera automatiquement à la liste blanche tous les numéros de téléphone utilisés pour envoyer des messages SMS ou MMS. Sélectionnez **Non** pour désactiver l'option.

- **Bloquer expéditeurs inconnus**. Si le paramètre est défini à **Non**, le composant Anti-Spam ne bloquera pas les messages entrants provenant de numéros de téléphone masqués. Choisissez **Oui** pour activer l'option.

- **Distinguer messages par type**. Si le paramètre est défini à **Non**, la valeur **Tous messages** sera utilisé pour le type de message des enregistrements créés dans la liste blanche ou noire (reportez-vous à la section 3.2.8.2 à la page 57 pour plus de détails sur les paramètres des enregistrements des listes) autrement, les nouveaux enregistrements seront créés selon le type de message spécifique (SMS ou MMS).

Ce paramètre affectera les enregistrements créés par le composant Anti-Spam uniquement dans les cas suivants :

- L'ajout de numéros sortants à la liste blanche (l'option **Autoriser les messages sortants** est active).
- L'ajout des numéros de téléphone d'où proviennent les nouveaux messages, à l'une des listes (voir section 3.2.8.4 à la page 61 pour plus de détails).

3.2.8.4. Actions appliquées aux messages

Quand vous recevez un message SMS ou MMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, le composant Anti-Spam intercepte le message et affiche le message correspondant (voir fig. 51).

Figure 51. Message du composant Anti-Spam

Vous pouvez utiliser le menu **Options** pour sélectionner et appliquer l'une des actions suivantes au message :

- **Ajouter à la liste blanche** – autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.

- **Ajouter à la liste noire** – bloque la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.

- **Ignorer le message** – autorise la réception du message. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Si le paramètre **Distinguer messages par type** de la configuration antipourriel est définit à **Non**, alors les actions **Ajouter à la liste blanche** ou **Ajouter à la liste noire** créeront respectivement un enregistrement pour tous les messages dans la liste correspondante (**Type de message** – **Tous messages**), autrement le type correspondra au type du message reçu. Reportez-vous à la section 3.2.8.2 à la page 57 pour plus de détails sur les paramètres des enregistrements de liste.

Des informations sur les messages bloqués sont ajoutées au rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Info** et sélectionnez **Rapports**.

3.2.9. Mise à jour des bases anti-virus

Kaspersky Anti-virus détecte les virus grâce aux enregistrements de ses bases anti-virus qui contiennent la description de tous les logiciels nocifs connus. Il est extrêmement important de protéger la sécurité de votre smartphone en mettant à jour fréquemment les bases anti-virus.

Vous pouvez lancer la mise à jour manuellement ou programmer son exécuter automatique à une heure spécifiée. Les mises à jour peuvent être téléchargées depuis les serveurs de mise à jour de Kaspersky Lab ou à partir d'un dossier local (voir section 3.2.9.1 à la page 63 à propos des méthodes de mise à jour).

Vous pouvez configurer l'application pour analyser automatiquement le système de fichiers du smartphone après chaque mise à jour. Pour ce faire, ouvrez la page **Mise à jour**, sélectionnez **Paramètres** et définissez l'option **Analyser après la mise à jour** à **Actif**.

Le paramètre **Analyser Quar. après mise à jour** permet d'activer ou désactiver l'analyse des objets en quarantaine après chaque mise à jour des bases anti-virus. L'analyse est activée par défaut. Pour la désactiver, sélectionnez **Inactif**.

Si vous ne souhaitez pas sélectionner un point d'accès lors de chaque mise à jour, donnez au paramètre **Demander le point d'accès** la valeur **Inactif**. Le programme mémorisera alors le dernier point d'accès utilisé avec succès et effectuera les mises à jour suivantes en se connectant au même point.

Le paramètre **Serveur de mise à jour** définit la source des mises à jour de la bases anti-virus : serveurs de mise à jour de Kaspersky Lab ou serveur spécifié par l'utilisateur. Si le paramètre est défini à **personnalisé**, la liste des options s'élargit pour en inclure une autre, le **nom de l'URL**. Vous pouvez spécifier un serveur alternatif, si nécessaire.

Pour afficher les informations sur la base de données en cours, ouvrez l'onglet **Info** et sélectionnez **Info base AV**.

Les informations de mise à jour sont enregistrées dans le rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Info** et sélectionnez **Rapports**.

3.2.9.1. Sélection de la méthode de mise à jour

Pour sélectionner l'origine des mises à jour, procédez de la manière suivante :

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).

2. Dans la page Mise à jour, sélectionnez Paramètres de mise à jour (voir fig. 52).

Figure 52. La page **Mise à jour**

3. Sélectionnez la source de la mise à jour :

- Mises à jour locales : l'application utilisera les mises à jour des bases disponibles dans votre smartphone. Pour sélectionner ce type de mise à jour, définissez la valeur à **Chercher dans le téléphone**.

- Mises à jour Web : l'application téléchargera les mises à jour à partir des serveurs de Kaspersky Lab. Pour sélectionner ce mode de mise à jour, définissez la valeur à **Mise à jour WAP**, pour utiliser WAP, ou à **Mise à jour HTTP** pour télécharger les mises à jour en utilisant le protocole HTTP. Sélectionnez **Avec navigateur** pour recevoir les mises à jour à l'aide du navigateur de votre smartphone.

Pour mettre à jour la base depuis Internet, votre smartphone doit disposer d'une connexion GPRS (pour la mise à jour via HTTP) ou une connexion WAP.

Si Kaspersky Anti-virus est configuré pour faire la mise à jour à partir d'un fichier local, copiez le fichier de la nouvelle base dans le smartphone par n'importe lequel des moyens habituels. Quand la mise à jour démarre, Kaspersky Anti-virus détecte automatiquement le fichier avec les bases les plus récentes et remplace l'ancien fichier par le nouveau.

Si vous sélectionnez la mise à jour en utilisant un navigateur Web, au démarrage de Kaspersky Anti-virus, celui-ci lancera le navigateur Web du smartphone, téléchargera les mises à jour et les recopiera automatiquement dans le répertoire de travail.

Si Kaspersky Anti-virus est configuré pour faire la mise à jour par Internet :

1. Activer / Désactiver la demande de point d'accès (paramètre Demander le point d'accès).

   Vous pouvez définir un point d'accès à partir des informations fournies par votre opérateur.

   Si vous sélectionnez **Inactif**, la connexion se réalisera en utilisant le dernier point d'accès utilisé pour la mise à jour.

   Si la demande est active, vous aurez à faire le choix dans une liste de point d'accès disponibles (voir fig. 53).

Figure 53. Sélection d'un point d'accès

2. Si nécessaire, utilisez la commande **Url de mise à jour** pour spécifier l'adresse du serveur de mise à jour.

Figure 54. URL du serveur de mise à jour

Par défaut, les mises à jour sont récupérées d'un serveur de Kaspersky Lab à l'adresse : http://ftp.kaspersky.com/index/mobile.xml.

La mise à jour sera suivie par la déconnexion Internet, même si la connexion était déjà établie.

3.2.9.2. Mise à jour manuelle

Pour lancer la mise à jour des bases anti-virus manuellement :

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).
2. Sélectionnez la source de la mise à jour (voir section 3.2.9.1 à la page 63).
3. Dans l'onglet Mise à jour sélectionnez Mise à jour maintenant (voir fig. 52).

3.2.9.3. Mise à jour programmée

Pour planifier les mises à jour des base anti-virus,

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).
2. Sélectionnez la source de la mise à jour (voir section 3.2.9.1 à la page 63).
3. Utilisez la page Mise à jour pour sélectionner Planification et configurez les paramètres de Mise à jour automatique :

    - **Quotidien** – exécute la mise à jour une fois par jour. Spécifiez l'**Heure de mise à jour automatique**.
    - **Hebdomadaire** – exécute la mise à jour une fois par semaine. Spécifiez le **Jour de mise à jour automatique** et l'**Heure de mise à jour automatique**.

3.2.10. Renouvellement de la licence

Pour rallonger la durée de votre licence d'utilisation du programme, procédez comme ceci :

1. Lancez Kaspersky Anti-virus (voir section 3.2.2 à la page 43).

2. Ouvrez le menu **Info**, sélectionnez **Licence** puis **Renouveler**.

3. Suivez les instructions de la section 3.2.1 à la page 41 pour saisir le nouveau code dans la fenêtre d'activation.

Vous pouvez également afficher des informations associées à la clé courante ainsi que sa période de validité avec la commande Info inscription du menu Licence KAV (voir fig. 50).

Figure 55. Gestion des licences

3.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

1. Sélectionnez la commande Supprimer du menu Applications. (voir fig 56).

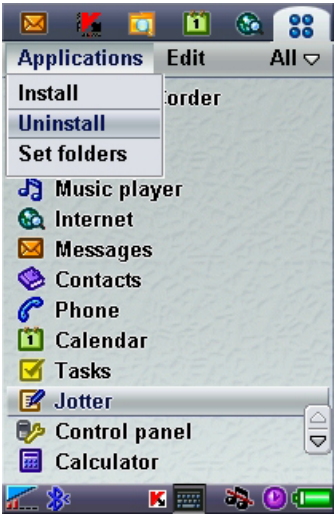

Figure 56. Démarrage de l'opération de suppression

2. Sélectionnez **KAV Mobile** dans la listes des applications installées. Cliquez ensuite sur Supprimer (voir fig. 57).

Figure 57. Sélection du programme à supprimer

3. Pour confirmer la suppression du programme, appuyez sur Oui (voir fig 58).

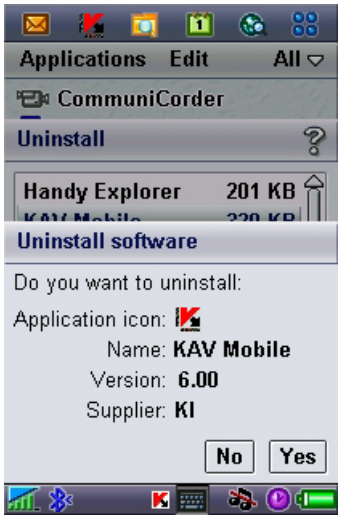

Figure 58. Confirmation de la suppression du programme

CHAPITRE 4. KASPERSKY ANTIVIRUS POUR SYMBIAN OS 7.0 SERIES 80 UI

Ce chapitre décrit le fonctionnement de Kaspersky Antivirus Mobile sur des smartphones exploités sous Symbian OS 7.0 Series 80 UI.

4.1. Installation de Kaspersky Anti-Virus

Pour installer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Copiez le paquet de distribution dans votre smartphone.

2. Exécutez l'installation (ouvrez le fichier CAB de la distribution dans le smartphone).

3. Lisez le texte du contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir fig. 59)[3].

[3] Toutes les captures d'écran de ce document correspondent à un smartphone modèle I-mate Nokia 9300 smartphone. Sur d'autres modèles de smartphones, l'interface de l'application peut varier.

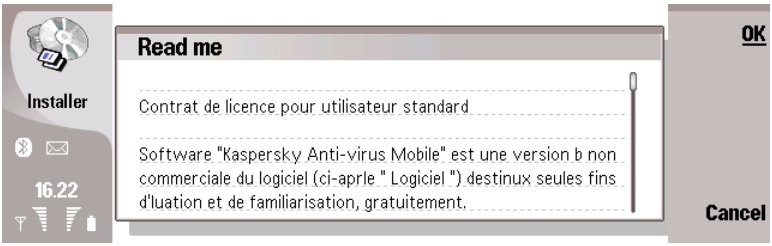

Figure 59. Gestion de la licence

4.2. Utilisation de l'application

Cette section décrit la configuration de l'anti-virus et de la protection en temps réel, le filtrage des messages SMS et MMS, l'analyse anti-virus du terminal et les mises à jour de l'application.

4.2.1. Activation du logiciel

Lors de son premier démarrage, le logiciel affiche une boîte de dialogue proposant d'activer Kaspersky Anti-virus (voir fig. 60).

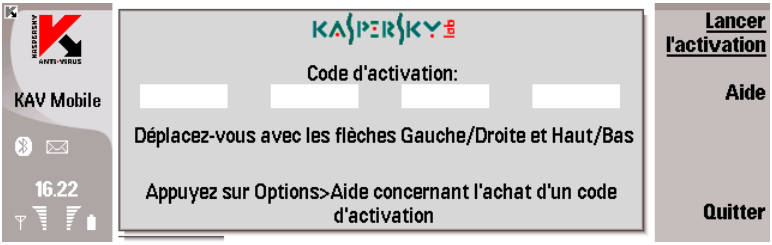

Figure 60. Fenêtre d'activation du programme

L'activation du programme est nécessaire pour autoriser toutes les fonctionnalités de Kaspersky Anti-virus. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab.

Attention !

Une connexion GPRS est nécessaire pour activer Kaspersky Anti-virus Mobile 6.0 sur un smartphone.

Le code d'activation est composé de lettres et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus. Utilisez les boutons « Haut/Bas » pour vous déplacer aux champs précédent ou suivant.

Après avoir saisi le code d'activation, choisissez la commande **Lancer l'activation**. L'application enverra une pétition HTTP à un serveur d'activation de Kaspersky Lab puis elle téléchargera et installera une clé de licence.

Si le code d'activation saisi s'avère être incorrect pour une raison ou une autre, le programme affiche un message correspondant.

4.2.2. Lancement de l'application

Pour lancer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Basculez sur le bureau du smartphone.
2. Sélectionnez l'icône *KAV Mobile*.
3. Appuyez sur **Ouvrir** pour démarrer l'application.

Après le démarrage de l'application, le smartphone affiche une fenêtre décrivant l'état des composants principaux de Kaspersky Anti-virus (voir fig. 61).

- **Protection en temps réel** – utilisation du mode de protection en temps réel (voir section 4.2.4.3xx).
- **Dernière analyse complète** – date et heure de la dernière analyse anti-virus du smartphone.
- **Date de la base de données** – date de publication de la base utilisée par l'application.
- **Config. Anti-Spam** – Mode d'exploitation du composant Anti-Spam utilisé pour filtrer les messages SMS.

Figure 61 Fenêtre d'état des composants de l'application

Pour commencer à utiliser l'application, appuyez sur **OK**.

4.2.3. Interface graphique utilisateur

L'interface graphique de l'application est formée par deux fenêtres (voir fig. 48xx), à savoir, la fenêtre principale de KAV Mobile (à gauche) et une fenêtre contenant cinq onglets (à droite) :

- L'onglet **Analyse** permet d'effectuer une analyse anti-virus du smartphone, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique.

- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.

- L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de modifier les paramètres et de planifier la mise à jour.

- L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS et MMS entrants.

- L'onglet **Info** permet d'afficher les rapports d'activité des composants de l'application, des informations générales sur l'application et la base anti-virus utilisée ; elle permet de modifier les paramètres généraux du fonctionnement de l'application et de gérer les licences.

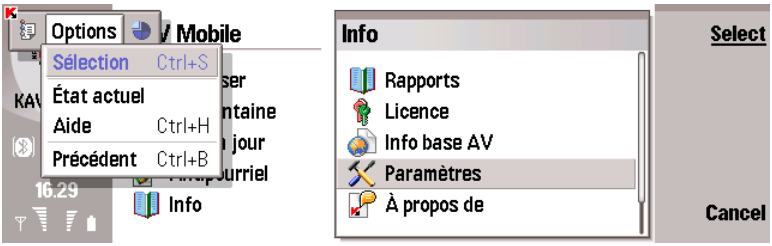

Figure 62. Fenêtre principale de **KAV Mobile**

Pour ouvrir l'onglet souhaité, sélectionnez son nom dans la fenêtre principale puis cliquez sur **Sélection**. Vous pouvez également basculer sur l'onglet souhaité à l'aide d'un joystick.

Pour revenir à la fenêtre d'état des composants logiciels, sélectionnez **État actuel** dans le menu **Fonctions**.

Pour quitter l'application, appuyez sur **Quitter** dans la fenêtre principale.

4.2.4. Analyse et protection antivirus

L'onglet **Analyse** permet d'effectuer une analyse anti-virus du système de fichiers complet et de la mémoire du smartphone ou seulement d'un fichier ou d'un répertoire individuel. Vous pouvez également modifier la configuration de l'analyse et du mode de protection anti-virus, afficher un rapport avec les résultats de l'analyse, ou planifier le démarrage automatique de l'analyse. Cette section décrit le fonctionnement de chacune de tâches précédentes.

4.2.4.1. Analyse à la demande

Kaspersky Anti-virus peut réaliser une analyse complète du système de fichiers de votre smartphone, y compris les objets présents sur les cartes d'extension mémoire connectées au téléphone.

Les résultats de l'analyse seront ajoutés au rapport. Vous pouvez afficher le rapport en sélectionnant **Affichage des rapports** sur l'onglet **Info**.

Pour modifier la configuration de l'analyse à la demande, procédez comme suit :

1. Sélectionnez **Paramètres** sur l'onglet **Analyse**.

2. Spécifiez le type des fichiers à analyser. Pour ce faire, sélectionnez **Type de fichier** et utilisez **Modifier** pour spécifier :

   - **Exécutable** – analyse uniquement les fichiers exécutables.

   - **Tous les fichiers** – analyse tous les types de fichiers

3. Spécifie l'action que l'application doit réaliser lors de la détection of d'un objet infecté, par la sélection de l'une des valeurs suivantes du paramètre **Action anti-virus** :

   - **Autosuppression** – supprime les objets infectés détectés

   - **Quarantaine** – place en quarantaine les objets infectés détectés

   - **Ask User** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté ou de le placer en quarantaine.

4. Spécifiez si l'analyse doit procéder à la décompression et analyse des archives SiS. Pour ce faire, sélectionnez Décompression LHA et ICE puis sélectionnez **Oui** ou **Non** à l'aide de **Modifier**.

Pour lancer une analyse anti-virus :

1. Lancez Kaspersky Anti-virus (voir section 4.2.2 à la page 72).

2. Sélectionnez **Analyse complète** sur l'onglet **Analyse** (voir fig. 62) si vous souhaitez analyser le système de fichiers complet de votre smartphone ou **Analyser dossier** pour analyser un dossier individuel.

   Quand l'option **Analyser dossier** est sélectionnée, une fenêtre présente alors le système de fichiers du smartphone. Pour lancer l'analyse sur un dossier, sélectionnez le dossier souhaité à l'aide du joystick puis cliquez sur **Sélection**.

Après démarrage de l'analyse, une fenêtre affiche l'état courant, le nombre d'objets analysés, le chemin de chaque objet et le pourcentage de progression de l'analyse (voir fig. 63).

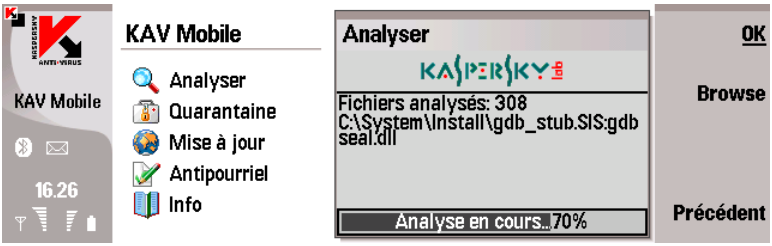

Figure 63. Fenêtre d'**analyse**

En cas de détection d'un objet infecté, l'application propose de supprimer le fichier concerné (action **Autosuppression**) ou de le déplacer vers la quarantaine (action **Déplacer vers quarantaine**).

Le logiciel ne demandera l'action à réaliser sur un objet que si le paramètre **Action anti-virus** est définit à **Demander** (voir plus haut).

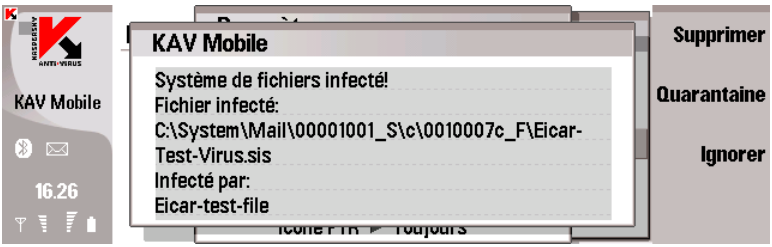

Figure 64. Notification de détection de virus

Une fois l'analyse terminée, l'application présente des statistiques générales sur le total d'objets analysés, la durée d'analyse et le nombre d'objets nocifs détectés, supprimés ou placés en quarantaine.

4.2.4.2. Planification de l'analyse

Kaspersky Anti-virus permet de planifier des analyses automatiques du smartphone à une heures programmée. L'analyse sera effectuée en arrière-plan. En cas de détection d'un objet infecté, l'application exécute l'action spécifiée par les paramètres d'analyse (voir section **Paramètres d'analyse**).

L'analyse programmée est désactivée par défaut.

Pour configurer une analyse planifiée, procédez de la manière suivante :

Utilisez la page **Analyser** pour sélectionner **Planification**, appuyez sur Sélection puis sélectionnez **Analyse auto** dans la fenêtre **Planification** ouverte (voir fig. 65). Utilisez **Modifier** pour sélectionner :

- **Hebdomadaire** – l'analyse s'exécutera chaque semaine. Le jour et l'heure d'analyse sont déterminés par les paramètres **Jour d'analyse auto** et **Heure d'analyse auto**.

- **Quotidien** – l'analyse s'exécutera tous les jours. L'heure d'analyse est déterminée par le paramètre **Heure d'analyse auto**.

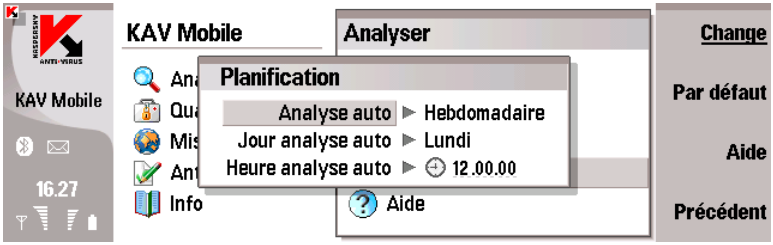

Figure 65. La fenêtre **Planification**

4.2.4.3. Protection en temps réel des fichiers

Dans le mode de protection en temps réel, la partie résidente de Kaspersky Anti-virus reste en permanence dans la mémoire de votre smartphone, pour surveiller toutes les données ou seulement les données entrantes (en fonction des paramètres sélectionnés).

Le mode de protection en temps réel reste activé depuis le démarrage jusqu'à l'arrêt du smartphone (à moins que ce mode ne soit désactivé par configuration).

Les informations de mise à jour sont enregistrées dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Information**.

Pour modifier la configuration de la protection en temps réel :

1. Sélectionnez **Paramètres** sur l'onglet **Analyse**.

2. Définissez la zone de protection en temps réel. Pour ce faire, sélectionnez **Protection en temps réel** et utilisez **Modifier** pour spécifier :

   - **Entrants seuls** – assure la protection en temps réel des objets entrants uniquement.

   - **Tout** – assure la protection en temps réel de tous les objets.

3. Spécifiez le type des fichiers à analyser. Pour ce faire, sélectionnez **Masque d'analyse** et utilisez **Modifier** pour spécifier :

   - **Exécutable** – analyse uniquement les fichiers d'application exécutables (par exemple: *.exe, *.sis, *.mdl, *.app).

   - **Tous les fichiers** – assure la protection en temps réel de tous les objets.

4. Définissez l'action à réaliser en cas de détection d'un objet infecté en sélectionnant l'une des valeurs du paramètre **Action anti-virus**.

   - **Autosuppression** – supprime les objets infectés détectés

   - **Quarantaine** – place en quarantaine les objets infectés détectés

   - **Demander** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté ou de le placer en quarantaine.

5. Spécifiez si la zone d'analyse doit inclure la RAM du smartphone qui, sous certaines circonstances, peut être vulnérable au logiciels nocifs. Pour ce faire, sélectionnez **Analyser ROM** et sélectionnez **Oui** ou **Non** à l'aide du bouton **Modifier**.

6. Spécifiez si l'analyse doit procéder à la décompression et analyse des archives SiS et ZIP. Pour ce faire, sélectionnez **Décompression LHA et ICE** et sélectionnez **Oui** ou **Non** à l'aide du bouton **Modifier**.

7. Configurez l'analyse des nouvelles cartes flash. Pour ce faire, sélectionnez cochez l'option **Analyser carte** et utilisez **Modifier** pour spécifier :

- **Demander** – afficher un message proposant d'analyser une carte flash après sa connexion.

- **Analyse auto.** – analyse toujours une carte flash lors de sa connexion.

8. Indiquez si l'icône Kaspersky Anti-virus doit être affichée. Pour ce faire, sélectionnez **Icône PTR** et utilisez **Modifier** pour spécifier :

   - **Toujours** – affiche toujours l'icône Kaspersky Anti-virus sur l'écran du smartphone.

   - **Jamais** – l'icône Kaspersky Anti-virus n'est jamais affiché.

4.2.5. Utilisation de la quarantaine

La quarantaine est une zone de stockage des objets infectés. Les objets infectés placés en quarantaine ne sont pas en mesure d'endommager votre smartphone et peuvent être supprimés ou restaurés par la suite.

Le logiciel peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Si vous souhaitez configurer l'application pour placer automatiquement en quarantaine les objets infectés détectés au cours d'une analyse à la demande ou en temps réel, ouvrez la page **Analyse**, sélectionnez **Paramètres** et définissez le paramètre **Action antivirus** à **Quarantaine**.

Si vous avez choisi l'action **Demander**, lors de la détection d'un objet infecté, Kaspersky Anti-virus vous proposera son effacement ou son déplacement en quarantaine.

Pour afficher le contenu de la Quarantaine, ouvrez l'onglet Quarantaine et sélectionnez Quarantaine (voir fig. 66).

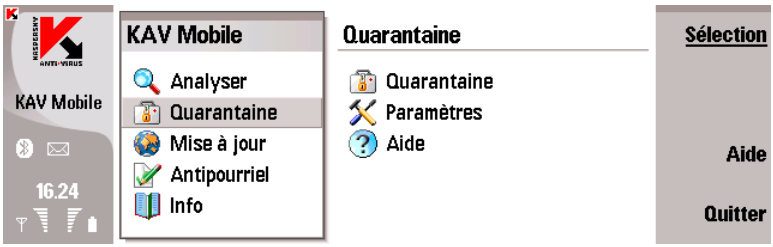

Figure 66. **Quarantaine**

Le menu **Options** de la fenêtre Quarantaine permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Détails**).
- Supprimer l'objet courant (**Supprimer fichier**).
- Purger la quarantaine en supprimant tous les objets conservés (**Tout supprimer**).
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer fichier**).

Vous pouvez également configurer la quarantaine. Pour ce faire, sélectionnez **Paramètres** sur l'onglet **Quarantaine**. Dans cette boîte de dialogue (voir fig. 67), configurez les paramètres suivants :

- **Taille de la quarantaine** – le nombre de fichiers conservés en quarantaine. Utilisez **Modifier** pour sélectionner 20, 50 ou 100 fichiers. La valeur par défaut est de 50 fichiers.
- **Conservation** – nombre de jours de conservation des objets en quarantaine. Utilisez **Modifier** pour sélectionner 7, 30 ou 60 jours, ou un délai indéterminé de conservation des fichiers (option **Illimité)**. La valeur de sélection par défaut est 60 jours.

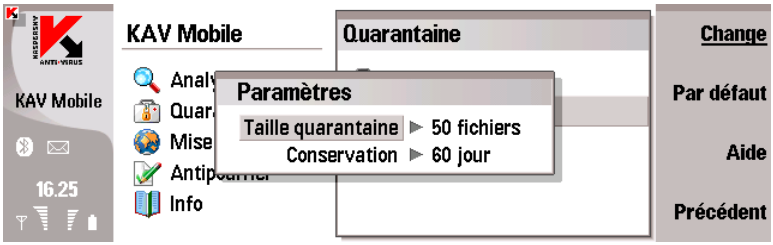

Figure 67. Configuration de la quarantaine

4.2.6. Utilisation du composant Anti-Spam

Le composant Anti-Spam est une nouvelle caractéristique de Kaspersky Antivirus Mobile 6.0. Il est destiné à protéger le smartphone contre les messages SMS et MMS indésirables.

Le principe utilisé pour filtrer les messages fait appel aux listes dites noire et blanche. Le composant Anti-Spam permet de bloquer les messages entrants provenant de numéros de téléphone ajoutés à votre liste noire. Les messages provenant de numéros ajoutés à la liste « blanche » ne seront pas bloqués.

Pour modifier la configuration du composant Anti-Spam :

1. Sélectionnez **Paramètres** sur l'onglet **Anti-Spam**.

2. Spécifiez si vous autorisez la réception de messages provenant de numéros de téléphone de votre liste de contacts. Pour ce faire, sélectionnez **Autoriser contacts** et sélectionnez **Oui** ou **Non** à l'aide du bouton **Modifier**.

3. Spécifiez si vous autorisez la réception de messages provenant de numéros de téléphone non inclus dans votre liste de contacts. Pour ce faire, sélectionnez **Bloquer inconnus** et sélectionnez **Oui** ou **Non** à l'aide du bouton **Modifier**.

4. Indiquez si vous souhaitez que l'application distingue les types de messages (SMS ou MMS) et si les règles antipourriel doivent s'appliquer à tous les messages, sans tenir compte de leurs types. Pour ce faire, sélectionnez **Distinguer msg par type** puis sélectionnez **Oui** ou **Non** avec **Modifier**.

5. Spécifiez si vous souhaitez ajouter les numéros de téléphone des messages sortants à la liste blanche. Pour ce faire, sélectionnez **Ajouter** sortants puis **Oui** ou **Non** à l'aide de la commande **Modifier**.

4.2.6.1. Modification des listes blanche et noire

La liste « noire » contient des numéros de téléphone dont la réception de messages est bloquée par le composant Anti-Spam.

La liste « blanche » contient des numéros de téléphone dont la réception de messages est autorisée.

Pour pouvoir modifier votre liste noire ou blanche, ouvrez la page **Anti-Spam** (voir fig. 68) et sélectionnez la liste souhaitée.

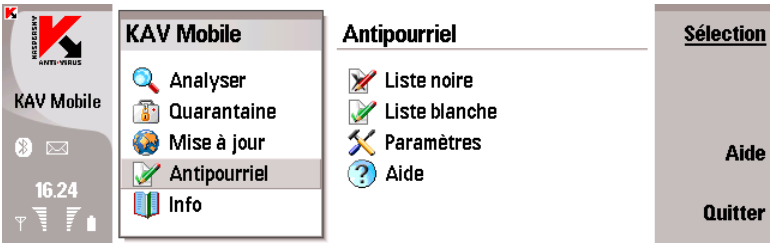

Figure 68. Le menu **Anti-Spam**

Pour modifier la liste utilisez le menu **Fonctions** :

- **Ajouter enregistrement** – ajoute un nouvel enregistrement dans la liste sélectionnée.
- **Modifier enregistrement** – modifie un enregistrement existant dans la liste.
- **Supprimer enregistrement**– supprime l'enregistrement courant de la liste.
- **Supprimer tout** – supprime tout

Après avoir sélectionné **Ajouter enregistrement**, spécifiez :

- le type de message provenant du numéro de téléphone spécifié, auquel les règles Anti-Spam seront appliquées. Cette option est disponible si le composant Anti-Spam est configuré pour faire la distinction entre types de messages (voir 4.2.6). Utilisez **Modifier** pour sélectionner **SMS seuls**, **MMS seuls** ou **Tous messages.**
- numéro de téléphone que vous souhaitez ajouter à la liste. Le numéro peut commencer par un chiffre ou par le signe « + » et ne peut contenir que des chiffres.

Après avoir modifié la liste, appuyez sur **Précédent** pour revenir à la page **Anti-Spam**.

4.2.6.2. Actions appliquées aux messages

Quand vous recevez un message SMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, et en supposant que vous avez autorisé la réception de messages provenant de numéros inconnus (voir section 4.2.6 à la page 80), le composant Anti-Spam affichera un avertissement sur l'écran du smartphone (voir fig. 69).

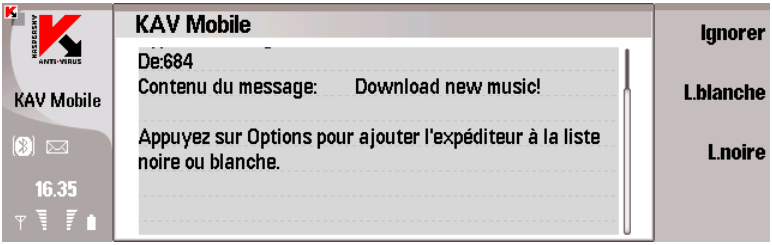

Figure 69. Avertissement du composant Anti-Spam

Dans le menu, choisissez l'une des actions suivantes à appliquer au message :

- **Ajouter à la liste blanche** – autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.

- **Ajouter à la liste noire** – bloque la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.

Pour autoriser la réception du message, appuyez sur **Ignorer**. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Des informations sur les messages bloqués sont ajoutées au rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Information**.

4.2.7. Mise à jour de la base antivirus

Kaspersky Anti-virus détecte les virus grâce aux enregistrements de sa base anti-virus, contenant la description de tous les logiciels nocifs connus. Il est extrêmement important de protéger la sécurité de votre smartphone en mettant à jour fréquemment les bases anti-virus.

Vous pouvez mettre à jour la base manuellement ou planifier l'opération. Pour configurer et démarrer la mise à jour, utilisez l'onglet **Mise à jour** (voir fig. 70). La mise à jour peut se faire par Internet depuis les serveurs de Kaspersky Lab, ou en local à partir du système de fichiers du smartphone.

Si la mise à jour se fait par Internet, elle sera suivie par une déconnexion, même si la connexion Internet était établie auparavant.

Figure 70. Onglet **Mise à jour**

Les informations de mise à jour de la base sont enregistrées dans le rapport. Vous pouvez afficher le rapport en sélectionnant **Rapports** sur l'onglet **Information**.

Pour lancer la mise à jour manuelle de la base anti-virus depuis les serveurs de Kaspersky Lab :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

2. Sélectionnez **Mise à jour** pour lancer l'opération de mise à jour.

Pour lancer la mise à jour de la base anti-virus depuis un dossier du système de fichiers du smartphone :

1. Téléchargez la nouvelle base anti-virus depuis les serveurs de Kaspersky Lab et déplacez les fichiers récupérés dans un dossier du système de fichiers du smartphone.

2. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

3. Dans la fenêtre ouverte, sélectionnez Paramètres puis définissez le **Type** de mise à jour**.** Appuyez sur **Arrière** pour enregistrer les paramètres et revenir à l'onglet **Mise à jour**.

4. Sélectionnez Mise à jour pour lancer le téléchargement de la mise à jour.

   Après cela, Kaspersky Anti-virus recherchera la base anti-virus dans le système de fichiers du smartphone. Après avoir détecté la base de données, celle-ce sera mise à jour automatiquement.

Pour planifier une mise à jour automatique de la base anti-virus :

1. Démarrer Kaspersky Anti-Virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

2. Sélectionnez **Planification** pour modifier la configuration de mise à jour automatique.

3. Utilisez **Modifier** pour indiquer la fréquence en modifiant la valeur du paramètre **Mise à jour automatique** :

   - **Quotidien** – exécute la mise à jour tous les jours. En outre, spécifiez l'**Heure** des mises à jour à réaliser.

   - **Hebdomadaire** – l'analyse est exécutée chaque semaine. En outre, spécifiez le Jour et l'Heure des mises à jour à réaliser.

4.2.8. Renouvellement de la licence

Pour rallonger la durée de votre licence d'utilisation du programme, procédez comme ceci :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91).

2. Ouvrez le menu **Info** et sélectionnez **Licence**.

3. Dans la fenêtre ouverte (voir fig. 64) spécifiez **Renouveler** (pour afficher les informations sur la licence courante, sélectionnez **Infos sur la clé**).

4. Suivez les instructions de la section 4.2.1 à la page 71) pour saisir le nouveau code dans la fenêtre d'activation.

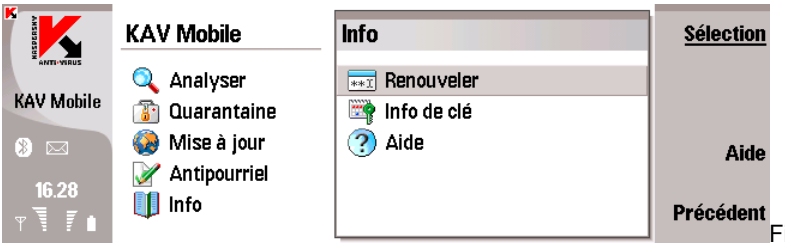

Figure 71. Gestion des licences

4.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

1. Sélectionnez Panneau de contrôle dans le menu Service (voir fig. 72).

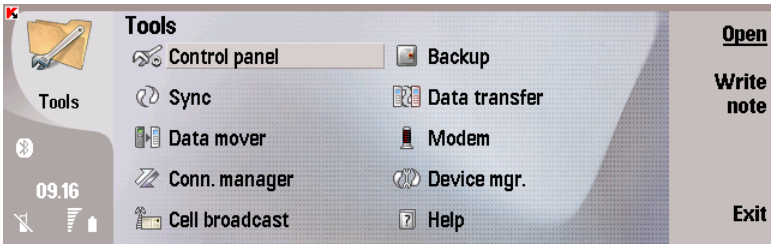

Figure 72. Ouverture du **Panneau de contrôle**

2. Dans la partie gauche de l'écran, sélectionnez Gestionnaire de données. Ensuite, dans la partie droite, sélectionnez Gestionnaire d'applications (voir fig. 73).

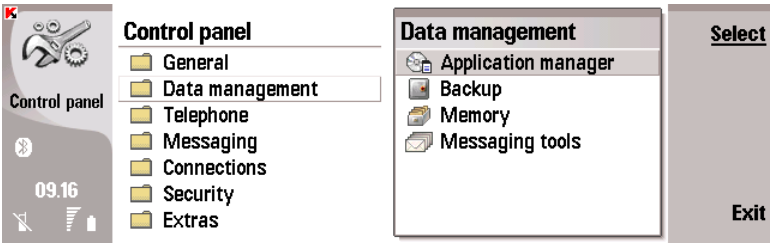

Figure 73. **Gestionnaire d'applications** - Démarrage

3. Sélectionnez KAV Mobile dans la listes des applications installées. Cliquez ensuite sur Supprimer (voir fig. 74).

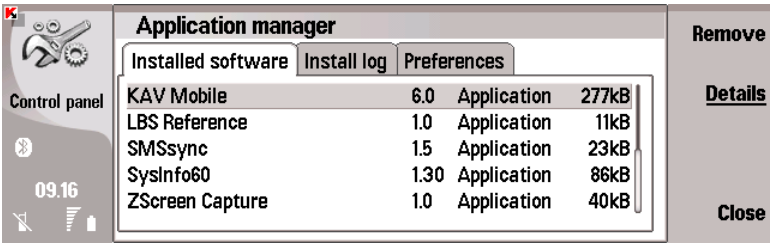

Figure 74. Choix d'une application

4. Cliquez sur **OK** dans la fenêtre d'avertissement (voir fig. 75).

Figure 75. Fin de la suppression

CHAPITRE 5. KASPERSKY ANTI-VIRUS POUR MICROSOFT WINDOWS MOBILE

Ce chapitre décrit le fonctionnement de Kaspersky Anti-virus Mobile sur des smartphones et des Pocket PC exploités sous l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 2003, 2003SE,
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

5.1. Installation de Kaspersky Anti-Virus

Pour installer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Copiez le fichier CAB contenant la distribution de l'application dans votre smartphone.
2. Exécutez l'installation (ouvrez le fichier CAB de la distribution dans le smartphone).

3. Lisez le texte du contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir fig. 76)[4].

Figure 76. Contrat de licence

5.2. Utilisation de l'application

Cette section décrit la configuration de l'anti-virus et de la protection en temps réel, le filtrage des messages SMS et MMS, l'analyse anti-virus du terminal et les mises à jour de l'application.

[4] Toutes les captures d'écran de ce document correspondent à un smartphone modèle I-mate K-JAM smartphone. Sur d'autres modèles de smartphones, l'interface de l'application peut varier.

5.2.1. Activation du logiciel

Lors de son premier démarrage, le logiciel affiche une boîte de dialogue proposant d'activer Kaspersky Anti-virus (voir fig. 77).

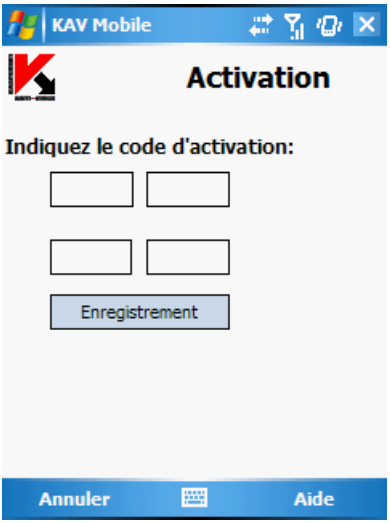

Figure 77. Boîte de dialogue d'activation du programme

L'activation du programme est nécessaire pour autoriser toutes les fonctionnalités de Kaspersky Anti-virus. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab.

Attention !

Une connexion GPRS est nécessaire pour activer Kaspersky Anti-virus Mobile 6.0 sur un smartphone.

Pour activer Kaspersky Anti-Virus sur un PDA, Microsoft Active Sync est nécessaire.

Le code d'activation est composé de lettres et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus. Utilisez les boutons « Haut/Bas » pour vous déplacer aux champs précédent ou suivant.

Après avoir saisi le code d'activation, choisissez la commande **Lancer l'activation** dans le menu **Options**. L'application enverra une pétition HTTP à un

serveur d'activation de Kaspersky Lab puis elle téléchargera et installera une clé de licence.

Si le code d'activation saisi s'avère être incorrect pour une raison ou une autre, le programme affiche un message correspondant.

5.2.2. Lancement de l'application

Pour lancer Kaspersky Anti-virus Mobile, procédez de la manière suivante :

1. Ouvrez le menu Applications du smartphone.

2. Sélectionnez l'icône  KAV Mobile et lancez l'application.

Après le démarrage de l'application, le smartphone affiche une fenêtre décrivant l'état des composants principaux de Kaspersky Anti-virus (voir fig. 78).

- **Dernière analyse complète** – date et heure de la dernière analyse anti-virus du smartphone.

- **Date de publication de la base –** date de publication de la base utilisée par l'application.

- **La protection en temps réel est actif/inactif** – état de la protection en temps réel. Pour plus de détails, voir section 5.2.4.3 à la page 98.

- **Anti-Spam actif/inactif** – Mode d'exploitation du composant Anti-Spam utilisé pour filtrer les messages SMS.

  Le composant Anti-spam n'est pas disponible pour le PDA.

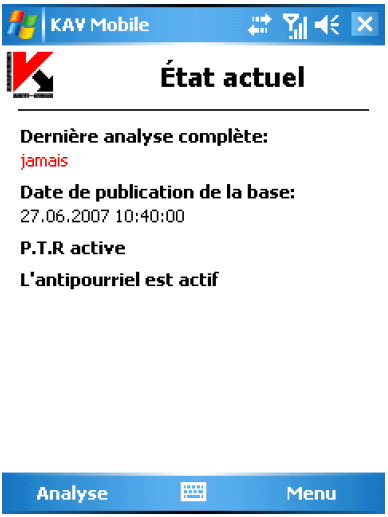

Figure 78 Fenêtre d'état des composants de l'application

5.2.3. Interface graphique utilisateur

L'interface graphique contient cinq onglets disponibles depuis le **Menu** (voir fig. 79) :

- L'onglet **Analyse** permet d'effectuer une analyse anti-virus du smartphone, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique.
- L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS et MMS entrants.
- L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de modifier les paramètres et de planifier la mise à jour.
- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.
- L'onglet **Info** permet d'afficher les rapports d'activité des composants de l'application, des informations générales sur l'application et la base anti-

virus utilisée, ainsi que de modifier les paramètres généraux de l'application.

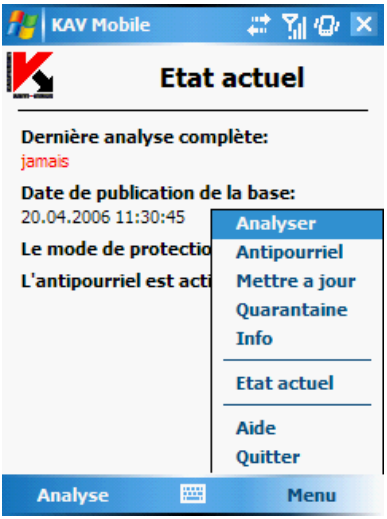

Figure 79. Menu de l'application

Pour revenir à la fenêtre d'état des composants de l'application, sélectionnez **Voir écran d'état**.

Pour quitter l'application choisissez **Quitter**.

5.2.4. Analyse et protection antivirus

L'onglet **Analyse** permet d'effectuer une analyse anti-virus du système de fichiers complet et de la mémoire du smartphone ou seulement d'un fichier ou d'un répertoire individuel. Vous pouvez également modifier la configuration de l'analyse et du mode de protection anti-virus, afficher un rapport avec les résultats de l'analyse, ou planifier le démarrage automatique de l'analyse. Cette section décrit le fonctionnement de chacune de tâches précédentes.

5.2.4.1. Analyse à la demande

Kaspersky Anti-virus peut réaliser une analyse complète du système de fichiers de votre smartphone, y compris les objets présents sur les cartes d'extension mémoire connectées au téléphone.

Les résultats de l'analyse seront ajoutés au rapport. Vous pouvez afficher le rapport en sélectionnant **Rapport d'analyse** sur l'onglet **Analyse**.

Pour modifier la configuration de l'analyse à la demande, procédez comme suit :

1. Sélectionnez Paramètres d'analyse sur l'onglet Analyse.

2. Spécifiez l'action que l'application doit réaliser lors de la détection of d'un objet infecté, par la sélection de l'une des valeurs suivantes du paramètre Action anti-virus :

    - **Demander** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté, de le placer en quarantaine ou de l'ignorer.

    - **Supprimer** – supprime les objets infectés détectés

    - **Quarantaine** – place en quarantaine les objets infectés détectés

    - **Ignorer** – ne réalise aucune action sur les objets infectés

Pour lancer une analyse anti-virus :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91).

2. Sélectionnez l'heure d'**Analyse complète** sur l'onglet **Analyser** (voir fig. 80) si vous souhaitez analyser le système de fichiers complet de votre smartphone ou **Analyser dossier** pour analyser un dossier individuel.

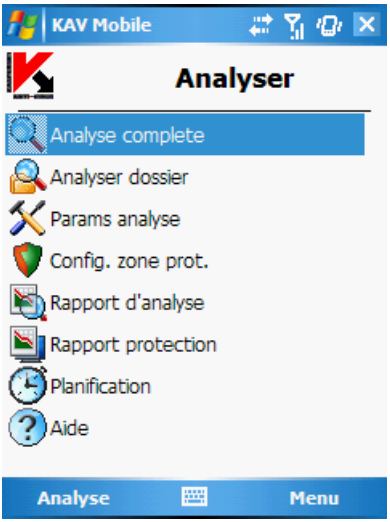

Figure 80. Onglet **Analyser**

Quand l'option **Analyser dossier** est sélectionnée, une fenêtre présente alors le système de fichiers du smartphone. Pour lancer l'analyse sur un dossier, déplacez le curseur vers le dossier concerné et appuyez sur **OK**.

Après le démarrage, une fenêtre affiche l'état courant, le nombre d'objets analysés et le chemin de chaque objet en cours d'analyse (voir fig. 81).

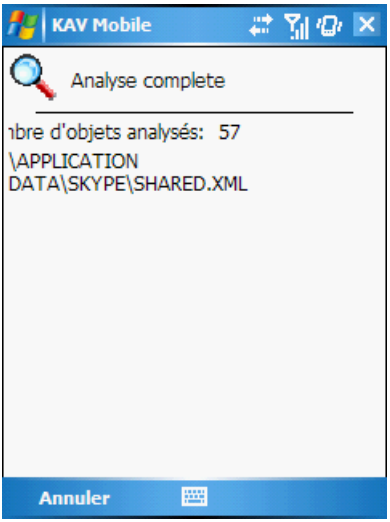

Figure 81. Fenêtre d'**analyse**

En cas de détection d'un objet infecté, l'application propose d'ignorer le fichier sans le modifier (**Ignorer**), de supprimer le fichier infecté (action → **Supprimer**) ou de le déplacer vers la quarantaine (action → **Quarantaine**).

Le logiciel ne demandera l'action à réaliser sur un objet que si le paramètre **Action anti-virus** est définit à **Demander** (voir plus haut).

Figure 82. Notification de détection de virus

Une fois l'analyse terminée, l'application présente des statistiques générales sur les objets malveillants détectés et supprimés.

5.2.4.2. Planification de l'analyse

Kaspersky Anti-virus permet de planifier des analyses automatiques du smartphone à une heures programmée. L'analyse sera effectuée en arrière-plan. En cas de détection d'un objet infecté, l'application exécute l'action spécifiée par les paramètres d'analyse (voir section **Paramètres d'analyse**).

L'analyse programmée est désactivée par défaut.

Pour configurer une analyse planifiée, procédez de la manière suivante :

Utilisez la page **Analyser** pour sélectionner **Planification** et configurez les paramètres **Analyse auto** (voir fig. 83) :

- **Quotidien** – l'analyse s'exécutera tous les jours. L'heure d'analyse est déterminée par le paramètre **Heure**.

- **Hebdomadaire** – l'analyse s'exécutera chaque semaine. Le jour et l'heure d'analyse sont déterminés par les paramètres **Jour de la semaine** et **Heure**.

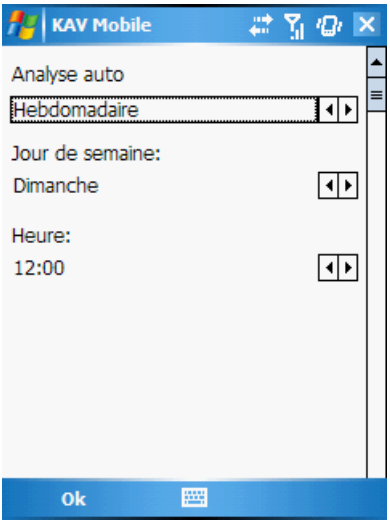

Figure 83. Le menu **Planification**

5.2.4.3. Protection en temps réel des fichiers

Dans le mode de protection en temps réel, la partie résidente de Kaspersky Anti-virus reste en permanence dans la mémoire de votre smartphone, pour surveiller toutes les données ou seulement les données entrantes (en fonction des paramètres sélectionnés).

Le mode de protection en temps réel reste activé depuis le démarrage jusqu'à l'arrêt du smartphone (à moins que ce mode ne soit désactivé par configuration).

Les résultats de l'analyse sont enregistrés dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapport de protection** dans l'onglet **Analyse**.

Pour modifier la configuration de la protection en temps réel :

1. Sélectionnez **Configuration de la zone protégée** sur l'onglet **Analyse**.

2. Activer / Désactiver la protection en temps réel en choisissant la valeur correspondante du paramètre **Protection en temps réel**.

3. Définissez l'action à réaliser en cas de détection d'un objet infecté en sélectionnant l'une des valeurs du paramètre **Action anti-virus**.

    - **Demander** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté, de le placer en quarantaine ou de l'ignorer.

    - **Supprimer** – supprime les objets infectés détectés

    - **Quarantaine** – place en quarantaine les objets infectés détectés

    - **Ignorer** – ne réalise aucune action sur les objets infectés

5.2.5. Utilisation de la quarantaine

La quarantaine est l'une de nouvelles caractéristiques introduites par Kaspersky Anti-virus® Mobile 6.0 après la version 1.7. Les objets infectés placés en quarantaine ne sont pas en mesure d'endommager votre smartphone et peuvent être supprimés ou restaurés par la suite.

Le logiciel peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Si vous souhaitez configurer l'application pour placer automatiquement en quarantaine les objets infectés, ouvrez la page **Analyser**, sélectionnez **Paramètres d'analyse** et définissez le paramètre **Action anti-virus** à **Quarantaine**.

Si vous avez choisi l'action **Demander**, lors de la détection d'un objet infecté, Kaspersky Anti-virus vous proposera son effacement ou son déplacement en quarantaine.

La page **Quarantaine** permet d'afficher le contenu de la quarantaine (voir fig. 84).

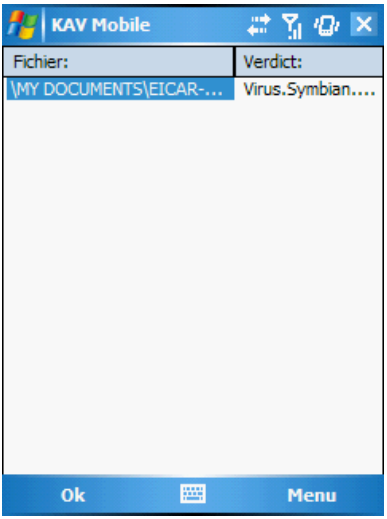

Figure 84. **Quarantaine**

Le menu **Options** de la fenêtre Quarantaine permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Détails**).
- Supprimer l'objet courant (**Supprimer**).
- Purger la quarantaine en supprimant tous les objets conservés (**Tout supprimer**).
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer**).

5.2.6. Utilisation du composant Anti-Spam

Le composant Anti-Spam est un autre caractéristique nouvelle introduite par Kaspersky Anti-virus Mobile 6.0. Il est destiné à protéger le smartphone contre les messages SMS et MMS indésirables.

Le composant Anti-spam n'est pas disponible pour le PDA.

Le principe utilisé pour filtrer les messages fait appel aux listes dites noire et blanche. Le composant Anti-Spam permet de bloquer les messages entrants provenant de numéros de téléphone ajoutés à votre liste noire. Les messages provenant de numéros ajoutés à la liste blanche ne seront pas bloqués.

Pour modifier la configuration du composant Anti-Spam :

1. Sélectionnez **Paramètres** sur l'onglet **Anti-Spam**.

2. Activer ou désactiver le composant Anti-Spam avec la case à cocher **Activer Anti-Spam**.

3. Spécifiez si vous autorisez la réception de messages SMS provenant de numéros de téléphone qui n'appartiennent à aucune des listes en cochant **Recevoir SMS : d'expéditeurs inconnus**.

4. Spécifiez si vous autorisez la réception de messages SMS provenant de numéros de téléphone de votre liste de contacts en cochant **Recevoir SMS : de ma liste de contacts**.

5.2.6.1. Modification des listes blanche et noire

La liste « noire » contient des numéros de téléphone dont la réception de messages SMS est bloquée par le composant Anti-Spam.

La liste « blanche » contient des numéros de téléphone dont la réception de messages SMS est autorisée.

Pour pouvoir modifier votre liste noire ou blanche, ouvrez la page **Anti-Spam** (voir Figure 85) et sélectionnez la liste souhaitée.

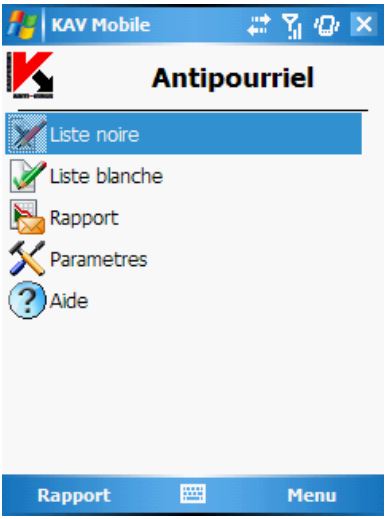

Figure 85. Menu **Anti-Spam**

Pour modifier la liste utilisez le **Menu** :

- **Ajouter enregistrement** – ajoute un nouvel enregistrement dans la liste sélectionnée.

- **Supprimer enregistrement** – supprime l'enregistrement courant de la liste.

Après avoir sélectionné **Ajouter enregistrement**, spécifiez le numéro de téléphone que vous souhaitez ajouter à la liste. Le numéro peut commencer par un chiffre ou par le signe "+" et ne peut contenir que des chiffres.

Après avoir modifié la liste, appuyez sur OK pour revenir à la page **Anti-Spam**.

5.2.6.2. Actions appliquées aux messages

Quand vous recevez un message SMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, et en supposant que vous avez autorisé la réception de messages provenant de numéros inconnus (voir section 5.2.6 à la page 100), le composant Anti-Spam affichera un avertissement sur l'écran du smartphone (voir fig. 86).

Figure 86. Avertissement du composant Anti-Spam

Utilisez **Menu** pour appliquer l'une des actions suivantes sur le message :

- **Ajouter à la liste blanche** – autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.
- **Ajouter à la liste noire** – bloque la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.

Pour autoriser la réception du message, appuyez sur **Ignorer**. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Des informations sur les messages bloqués sont ajoutées au rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Anti-Spam** et sélectionnez **Rapport**.

5.2.7. Mise à jour de la base antivirus

Kaspersky Anti-virus détecte les virus grâce aux enregistrements de sa base anti-virus, contenant la description de tous les logiciels nocifs connus. Il est extrêmement important de protéger la sécurité de votre smartphone en mettant à jour fréquemment les bases anti-virus.

Vous pouvez mettre à jour la base manuellement ou planifier l'opération. Pour configurer et démarrer la mise à jour, utilisez l'onglet **Mise à jour** (voir fig. 87). La mise à jour peut se faire par Internet depuis les serveurs de Kaspersky Lab, ou en local à partir du système de fichiers du smartphone.

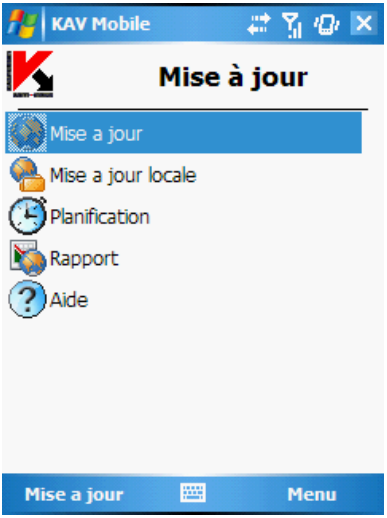

Figure 87. L'onglet **Mise à jour**

Les informations de mise à jour de la base sont enregistrées dans le rapport. Pour afficher le rapport, passez dans l'onglet **Mise à jour** et sélectionnez **Rapport**.

Pour lancer la mise à jour manuelle de la base anti-virus depuis les serveurs de Kaspersky Lab :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

2. Sélectionnez **Mise à jour** pour lancer l'opération de mise à jour.

Pour lancer la mise à jour de la base anti-virus depuis un dossier du système de fichiers du smartphone :

1. Téléchargez la nouvelle base anti-virus depuis les serveurs de Kaspersky Lab et déplacez les fichiers récupérés dans un dossier du système de fichiers du smartphone.

2. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

3. Sélectionnez **Mise à jour locale** et, dans la fenêtre ouverte, déplacez-vous jusqu'au dossier contenant les fichiers mis à jour.

Pour planifier une mise à jour automatique de la base anti-virus :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 91) et ouvrez l'onglet **Mise à jour**.

2. Sélectionnez **Planification** pour modifier la configuration de mise à jour automatique.

3. Spécifiez la fréquence des mises à jour en modifiant la valeur du paramètre **Mise à jour automatique** :

   - **Quotidien** – exécute la mise à jour tous les jours. En outre, spécifiez l'**Heure** des mises à jour à réaliser.

   - **Hebdomadaire** – l'analyse est exécutée chaque semaine. En outre, spécifiez le **Jour de la semaine** et l'**Heure** des mises à jour à réaliser.

   - **Mensuel** – exécute la mise à jour tous les mois. En outre, spécifiez le **Jour du mois** et l'**Heure** des mises à jour à réaliser.

5.2.8. Renouvellement de la licence

Pour rallonger la durée de votre licence d'utilisation du programme, procédez comme ceci :

1. Lancez Kaspersky Anti-virus (voir section 5.2.2 à la page 72).

2. Ouvrez le menu **Info** et sélectionnez **Activer** (voir fig. 88).

3. Suivez les instructions de la section 5.2.1 à la page 90) pour saisir le nouveau code dans la fenêtre d'activation.

Figure 88. Gestion des licences

5.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

1. Désactivez l'autoprotection (voir 5.2.4.3 à la p. 98 pour plus de détails) ;

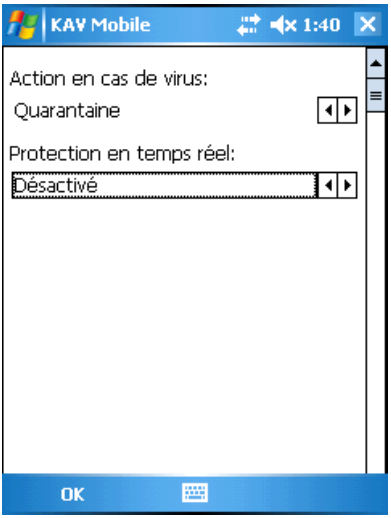

Figure 89. Désactiver l'autoprotection

2. Quittez Kaspersky Anti-Virus. Pour ce faire, sélectionnez Quitter dans le menu du programme (voir fig. 90).

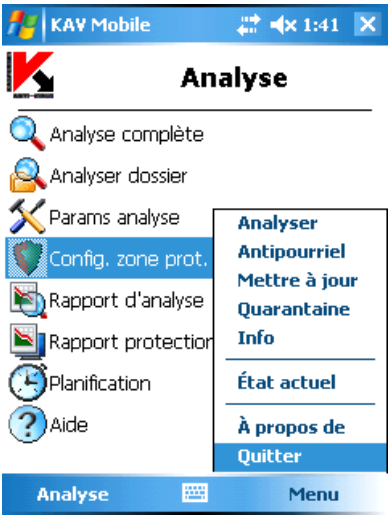

Figure 90. Sortie du logiciel

3. Supprimez le programme. Pour ce faire :

- Cliquez sur **Démarrer**, choisissez Paramètres puis sélectionnez **Suppression de programme** (voir fig. 91) :

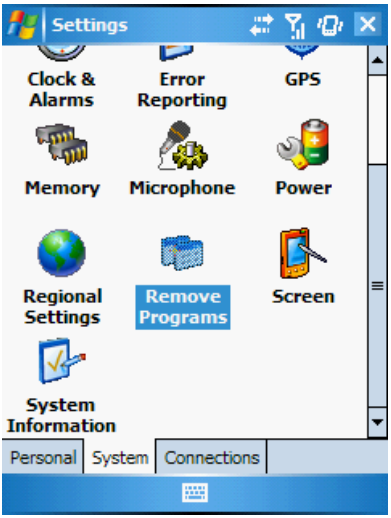

Figure 91. Démarrage de la suppression du logiciel

- Sélectionnez **KAV Mobile** dans la listes des applications installées puis sélectionnez **Supprimer** (voir fig. 92).

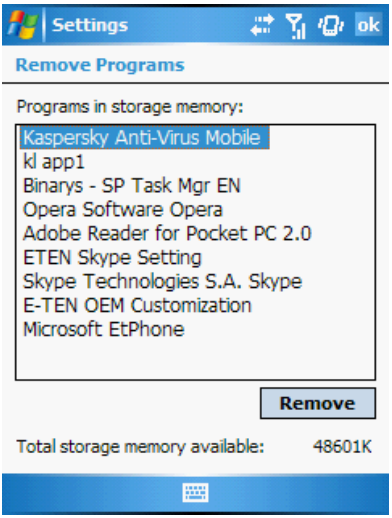

Figure 92. Sйlection du programme

- Pour confirmer la suppression, cliquez sur **Oui** (voir fig. 93).

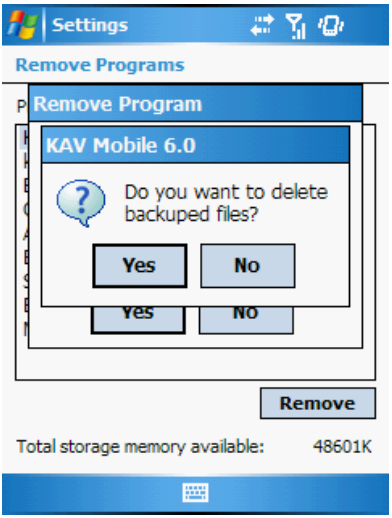

Figure 93. Confirmation de la suppression du programme

ANNEXE A. 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, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. 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 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. 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 améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. 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 Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne),

Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nos bases sont actualisées toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

A.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la “météo” des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d’informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S’abonner et se désabonner aux canaux d’information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d’informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l’information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.

- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.

- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.

- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.

- **Le contrôle des processus cachés** permet de lutter contre les Rootkit qui cachent le code malveillant dans le système d'exploitation.

- **Analyseur heuristique**. Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.

- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!

- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.

- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.

- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;

- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;
- *Génération de rapports détaillés* ;
- *Mise à jour automatique des bases* de l'application.

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable.* ;
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Blocage des fenêtres pop up et des bannières publicitaires* pendant la navigation sur Internet ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Outils de création d'un disque de démarrage* capable de restaurer le système après une attaque de virus ;

- *Système développé de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables* (technologie Intel® Centrino® Duo pour ordinateurs portables) ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Répartition de la charge entre les processeurs du serveur* ;
- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;

- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;

- *Analyse du courrier électronique et du trafic Internet* en temps réel ;

- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;

- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;

- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;

- *Isolement des objets suspects* dans un répertoire spécial ;

- *Mise à jour automatique des bases*.

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers* ;

- *Protection des serveurs de messagerie Sendmail, Qmail, Posftix et Exim* ;

- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;

- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;

- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;

- *Prévention des épidémies de virus et des diffusions massives* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Utilisation sécurisée des réseaux sans fil* Wi-Fi ;
- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes dans le système* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;

- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;

- *Protection des serveurs de messagerie et des serveurs de coopération* ;

- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;

- *Blocage de l'accès depuis un poste de travail infecté* ;

- *Prévention des épidémies de virus* ;

- *Rapports centralisés* sur l'état de la protection ;

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;

- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;

- *Compatibilité avec les serveurs proxy matériels* ;

- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;

- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;

- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;

- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;

- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™);
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Filtrage des messages non sollicités* ;

- *Analyse des messages et des pièces jointes du courrier entrant et sortant* ;
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Filtrage des messages* en fonction du type de pièce jointe ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* du logiciel ;
- *Prévention des épidémies de virus* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Système de rapports* sur l'activité de l'application ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Analyse du trafic Internet* (HTTP/FTP) en temps réel ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* ;
- *Système de rapports sur le fonctionnement de l'application* ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

A.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://kb.kaspersky.fr/faq.php
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://kb.kaspersky.fr/hq.php E-mail : info@fr.kaspersky.com

ANNEXE B. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD/DVD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD/DVD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la licence d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 *Utilisation*. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD/DVD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Il est interdit de transmettre le code d'activation et le fichier de clé de licence à un tiers. Le code d'activation et le fichier de clé de licence sont des informations strictement confidentielles.

1.1.7 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD/DVD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.