

SMS 007

Software pro ochranu komunikací – stručná uživatelská příručka

Obsah

Úvod.....	3
Vydání systému.....	3
Šifrování.....	3
Upozornění.....	4
Snímky obrazovky.....	4
Spuštění a ukončení aplikace.....	5
Hlavní nabídka aplikace.....	6
Kontakty.....	6
Zprávy.....	6
Nastavení.....	6
Zavřít	6
Seznam kontaktů.....	7
Implicitní skupina „Vše“.....	7
Další skupiny.....	7
Otevírání a zavírání skupin.....	7
Založení nového kontaktu.....	8
Doporučovaná délka hesel.....	8
Úprava kontaktu.....	11
Odeslání zprávy kontaktu nebo skupině.....	12
Odeslání kontaktu.....	12
Mazání kontaktu.....	12
SMS 007 Manager – rozšiřující schopnosti v seznamu kontaktů.....	12
Zprávy.....	14
Výpis zpráv, typy zpráv a jejich barevné označení.....	14
Hromadné mazání.....	14
Psaní nové zprávy.....	14
Volba adresáta.....	15
Odesílání zprávy.....	15
Přísně tajné zprávy.....	16
Maximální délka zprávy a počet zpráv.....	16
Čtení zpráv.....	16
Zatřídění zprávy do skupin.....	17
Archivace zpráv.....	17
Nastavení.....	18
Heslo aplikace.....	18
Zprávy.....	18
Paměť.....	18
Start aplikace.....	18
O aplikaci.....	19
Nápověda.....	19
Místní nastavení.....	19
Poznámky na závěr.....	20
Chyby výrobců.....	20
Zavírání aplikace.....	20

Úvod

SMS 007 je systém pro výměnu bezpečných (šifrovaných) SMS mezi dvěma uživateli. S použitím systému SMS 007 je možno si psát zcela bezpečné, nerozluštitelné zprávy, jejichž text nemůže být odposlechnut či zaznamenán, a to ani mobilním operátorem.

Sítí operátora procházejí zprávy v zašifrované podobě, a původní text je dostupný jen odesílateli a příjemci zprávy. Bližší informace naleznete na WWW stránkách <http://www.sms007.cz>.

SMS 007 je software pro mobilní telefony, určený pro platformu Java (J2ME) MIDP-2.0. Nepoužívá žádné funkce specifické pro nějaký typ telefonu, a tak by měl běžet na každém telefonu podporujícím technické standardy MIDP-2.0 a WMA (Wireless Messaging API).

Tato uživatelská příručka má být stručným návodem k použití aplikace „SMS 007“. Příručka nepopisuje instalaci produktu. Informace o instalaci naleznete na Webových stránkách www.sms007.cz.

Vydání systému

Systém SMS007 existuje v několika vydáních, která se liší číselným označením. Pozdější vydání mohou být vybavena vlastnostmi, které dřívější vydání nemají. U takových vlastností je v manuálu připojen komentář.

Současná vydání:

<i>Číselné označení</i>	<i>Vlastnosti tohoto vydání</i>
1.0.2	Neveřejné testovací vydání.
1.0.3	První veřejné vydání, 12.9.2005.
1.0.4	Vylepšené vydání, 30.9.2005.
1.0.5	Rozšiřující vydání, 14.10.2005 - podpora telefonů Motorola řady Vxxx a úprava ukončování aplikace.
1.0.6	Verze SMS 007 Manager, 10.1.2006
1.0.7	Verze SMS 007 Basic, určená pro mezinárodní trh, 8.2.2006

Šifrování

Nejen posílané zprávy, ale všechna citlivá data¹, která aplikace „SMS 007“ ukládá do telefonu, jsou chráněna šifrováním. To představuje ochranu pro případ, že někdo Váš telefon odcizí a bude zkoumat uložená data.

K šifrování uložených citlivých dat je používána symetrická šifra AES.

¹ Tj. interní seznam kontaktů, doručené, rozepsané a odeslané zprávy, skupiny kontaktů a zpráv, nastavení a hesla.

K odvozování klíčů z hesel je používána hashovací funkce SHA-2.

Upozornění

Ke každé obrazovce programu patří ovládací prvky – tlačítka s příkazy. Standardně dokáže telefon zobrazit tři ovládací prvky k jedné obrazovce – jeden k levému, jeden k prostřednímu a jeden k pravému tlačítku. V případě, že ovládacích prvků je více než 3, umístí se ke tlačítkům jen některé z nich a zbylé jsou umístěny do nabídky přístupné pod příkazem pojmenovaným „Volby“ (Nokia 6230; u jiných telefonů může být pojmenování jiné), který bývá nejčastěji dostupný na levém tlačítku.

Telefon může přidat k obrazovce svoje vlastní příkazy. Například Nokia 6230 přidává k obrazovkám s editací textu příkaz „Vložit smajlík“. Nad těmito příkazy nemají tvůrci programů žádnou kontrolu. Rovněž nemají definitivní kontrolu nad tím, jak budou příkazy po obrazovce rozmístěny – i to je v pravomoci telefonu samotného. V případě, že rozmístění příkazů vypadá na některé obrazovce nelogicky, není možno je zásadně změnit – telefon je automat a nechápe význam příkazů, které rozmisťuje.

Telefony Siemens série 65 rozmisťují příkazy i na prostřední tlačítko, kde se obvykle místo plného textu zobrazí jen první písmeno příkazu.

Příkazy přidávané automaticky telefonem nejsou v této příručce komentovány.

Snímky obrazovky

Snímky obrazovky v tomto manuálu byly pořízeny na přístroji Nokia 6600. Vzhled obrazovky na vašem telefonu se může od těchto snímků lišit.

Spuštění a ukončení aplikace

Po instalaci do telefonu se aplikace SMS 007 nachází v seznamu nainstalovaných aplikací. Přesné umístění se může lišit v závislosti na typu telefonu.

Příklady:

1. telefony Nokia Series 40 (např. Nokia 6230) mají v hlavním menu zvláštní položku „Aplikace“, v níž se nachází další položka „Sbírka“, a v ní již SMS 007;
2. telefony Nokia Series 60 (např. Nokia 6600) obvykle obsahují SMS 007 přímo v hlavním menu;
3. telefony Nokia Series 80 (Communicator) dávají uživateli možnost zvolit si umístění aplikace již v rámci instalace;
4. telefony Siemens obvykle obsahují SMS 007 v rámci položky „Zábava / Aplikace“

Spuštění aplikace probíhá tak, že naleznete umístění aplikace, najedete kurzorem na „SMS 007“ a stisknete „Otevřít“.

Spuštěnou aplikaci lze kdykoliv uzavřít červeným tlačítkem (ukončení hovoru), avšak mělo by se tak dít jen v následujících situacích:

1. dosud jste se nepřihlásili (tj. nezadali jste správné heslo)
2. nebo potřebujete aplikaci nutně „zabít“ (neodpovídá na Vaše příkazy, někdo cizí Vám hledí přes rameno apod.)

Ve všech ostatních situacích použijte k vypnutí aplikace volbu „Zavřít“ v hlavní nabídce spuštěné aplikace. Při vypnutí „červeným tlačítkem“ je aplikace ukončena dosti „tvrdě“ (nečeká se na dobehnutí některých procesů) a nemuselo by dojít k zápisu všech změněných dat.

Po spuštění aplikace se objeví jedna ze dvou následujících obrazovek:

1. volba hesla
2. přihlášení

Volba hesla se objeví, jen pokud heslo ještě nebylo nikdy zvoleno. V takovém případě zvolte heslo dlouhé minimálně 8 znaků, zadejte jej shodně do obou políček a zvolte Volby-OK. V případě, že jej nezadáte dvakrát stejně, Vás aplikace upozorní a bude trvat na volbě stejných hesel.

Buďte si jisti, že zvolené heslo není snadno uhodnutelné, a že jej nezapomenete. V případě, že byste heslo zapomněli, ztratíte navždy přístup ke svým datům!

Přihlášení se objeví, pokud už heslo bylo zvoleno. Zadejte správně heslo a zvolte Volby-OK. Pokud jej nezadáte správně, bude aplikace trvat na zadání správného hesla. Počet pokusů není v této verzi limitován.

V případě, že se nyní nechcete přihlásit, stiskněte červené tlačítko a aplikace bude ukončena.

V případě, že zadáte správné heslo, objeví se hlavní nabídka aplikace.

Hlavní nabídka aplikace

Hlavní nabídka aplikace se skládá z těchto položek:

1. Kontakty
2. Zprávy
3. Nastavení
4. Zavřít

Kontakty

Toto je vstupní brána k seznamu kontaktů aplikace. Sem vstupte, chcete-li:

- číst seznam kontaktů
- upravovat seznam kontaktů
- odeslat zprávu/zprávy osobám ze seznamu kontaktů
- odeslat kontakt na člověka jinému člověku

Podrobný popis seznamu kontaktů následuje v kapitole „Seznam kontaktů“.

Zprávy

Toto je vstupní brána ke čtení zpráv a k některými jejich úpravám. Sem vstupte, chcete-li:

- číst doručené nebo odeslané zprávy
- mazat či upravovat zprávy
- přeposílat doručené zprávy jiným osobám
- napsat novou zprávu osobě, kterou nemáte v seznamu kontaktů.

Podrobný popis zacházení se zprávami následuje v kapitole „Zprávy“.

Nastavení

V rámci „Nastavení“ se nacházejí další položky (podle vydání a verze až sedm). Sem vstupte, chcete-li provádět úpravy chování aplikace, např.:

- změnit heslo aplikace
- změnit chování automatického mazače
- změnit chování při startu aplikace

Podrobný popis nastavení následuje v kapitole „Nastavení“.

Zavřít

Stisknutím tohoto tlačítka ukončíte aplikaci. Toto je standardní způsob ukončování aplikace a je vhodné dávat mu přednost před „červeným tlačítkem“, které aplikaci ukončuje násilněji.

Seznam kontaktů

V běžných telefonech není možno přistupovat zevnitř Java aplikace k uloženému seznamu kontaktů. Výjimku tvoří telefony podporující tzv. PIM rozhraní, kterých je velmi málo. Pro tyto telefony existuje speciální verze – SMS 007 Manager.

Z tohoto důvodu udržuje aplikace SMS 007 svůj vlastní vnitřní seznam kontaktů. Má to i tu výhodu, že pokud se telefon dostane do ruky nepovolané osobě (a ta nezná hlavní heslo aplikace), nemá tato osoba šanci zjistit „citlivé položky“ ve Vašem seznamu kontaktů – v běžném seznamu kontaktů se totiž nebudou nacházet, a vnitřní seznam aplikace je chráněn šifrováním.

Pokud zvolíte „Kontakty“ z hlavní nabídky aplikace, dostanete se na seznam kontaktů. Seznam kontaktů obsahuje kontakty utříděné do skupin. Po instalaci je seznam kontaktů prázdný a obsahuje pouze prázdnou skupinu „Vše“.

Příkazy dostupné v rámci seznamu kontaktů jsou tyto:

Poslat – otevře obrazovku pro psaní nové zprávy kontaktu nebo skupině.

Přidat – otevře obrazovku pro přidání nového kontaktu.

Odeslat kontakt – otevře obrazovku pro odeslání kontaktu někomu jinému.

Upravit – otevře obrazovku pro změnu údajů kontaktu nebo pro přejmenování skupiny.

Smazat – provede smazání kontaktu nebo skupiny.

Nová skupina – otevře obrazovku pro založení nové skupiny.

Volat – jen u verze SMS 007 Manager, viz dále.

Přidat z kontaktů – jen u verze SMS 007 Manager, viz dále.

Implicitní skupina „Vše“

Skupina „Vše“, která se vždy nachází na prvním místě seznamu, je tzv. implicitní skupinou, do níž budou vkládány všechny nově tvořené kontakty. Skupinu „Vše“ není možno smazat, ale je možno ji prakticky libovolně přejmenovat (včetně prázdného jména).

Další skupiny

Uživatel si může založit dalších až 60 skupin kontaktů. Jedinou podmínkou je, aby se zakládaná skupina nejmenovala stejně jako nějaká existující. Jména skupin mohou obsahovat diakritiku (znaky s háčky a čárkami).

Po vytvoření je nová skupina prázdná (neobsahuje žádné kontakty).

Uživatel může existující skupinu přejmenovat nebo smazat. V případě přejmenování je jedinou podmínkou, aby skupina daného jména ještě neexistovala (nelze mít dvě skupiny téhož jména).

Přiřazení nějakého kontaktu do skupiny je možno při jeho zakládání nebo úpravách. Jeden kontakt může patřit do libovolného počtu skupin.

Otevírání a zavírání skupin

Skupiny kontaktů je možno stisknutím otevírat nebo zavírat. To je užitečná vlastnost pro orientaci v dlouhém seznamu kontaktů.

Zavřená skupina kontaktů je vyznačena „mřížemi“ v ikoně, otevřená skupina „mříže“ nemá.

Založení nového kontaktu

Založit nový kontakt je možno pomocí volby „Přidat“ v rámci seznamu kontaktů. Otevře se obrazovka, na níž je možno vyplnit údaje o kontaktu. Tučně označené údaje jsou povinné:

Jméno – neprázdné.

Telefon – neprázdný, začínající mezinárodní předvolbou (např +420608111111).

E-mail – může být prázdný

Heslo – neprázdné, aspoň 6 znaků (viz dále)

Heslo znovu - neprázdné, aspoň 6 znaků, stejné jak „Heslo“

Poznámka – může být prázdná, max. 150 znaků.

Šifrovat – volba typu šifry

V případě, že existují nějaké uživatelské skupiny, bude následovat jejich „zaškrtačkový“ seznam, v němž si můžete zvolit, do jakých skupin chcete nový kontakt zařadit. Přímou v rámci zakládání nového kontaktu je možno založit novou skupinu: Volby-Nová skupina.

Heslo je heslem, na jehož základě budou šifrovány zprávy mezi Vámi a zmíněným kontaktem. Toto heslo si domluvíte s člověkem, jehož kontakt vytváříte, a oba jej vyplníte do svých aplikací shodně. Nebudou-li se hesla v obou aplikacích shodovat, nebude možno rozluštit zprávy od dotyčné osoby. Doporučujeme, abyste si pro různé kontakty volili různá hesla. **Hesla si nemusíte pamatovat;** aplikace si ukládá jejich šifrované hashe (jsou chráněny před přečtením pomocí šifrování).

Čím komplikovanější heslo, tím lépe. Například „6jmaS%sdkjzb“ je lepší než „rollingstone“. Jelikož tato hesla si nemusíte pamatovat, volte je co nejsložitější.

V případě, že nezadáte mezinárodní předvolbu (+420), aplikace Vás na to upozorní a automaticky ji doplní. Zkontrolujte, zda se tak stalo správně, a zvolte znovu „OK“.

V případě, že se pokusíte založit kontakt s telefonním číslem, které je už nastaveno u jiného kontaktu, aplikace Vás na to upozorní. Je to ochrana před tím, abyste měli v telefonu jedno číslo pod dvěma různými jmény.

Kontakt založíte volbou „OK“. Pokud si přejete odejít z obrazovky bez uložení kontaktu, stiskněte „Zpět“. To je ostatně obecný princip ovládání aplikace.

Doporučovaná délka hesel

Komunikační hesla, nastavovaná při zakládání kontaktu, jsou velmi důležitá pro Vaši bezpečnost. Útočník, který sleduje provoz na síti a vidí Vaši zašifrovanou komunikaci, musí uhodnout komunikační heslo, aby se dostal k textu zprávy.

Protože komunikační hesla si nemusíte pamatovat, měli byste je volit co nejnáhodnější – **nikdy nepoužívejte normální slova žádného jazyka, ani smysluplné kombinace písmen!** Hesla by měla zahrnovat velká písmena, malá písmena, číslice a nějaké speciální symboly (jako %, #, !). Nepoužívejte písmena s háčky a čárkami, neboť jejich podoba v různých telefonech může být různá, a mohly by vzniknout problémy s šifrovanou komunikací.

Pokud je komunikační heslo zkonstruováno tímto postupem, je u každého znaku zhruba 64

možností (27 velkých písmen, 27 malých písmen, 10 číslic a několik zvláštních znaků. Budeme používat odhad 64, neboť jde o mocninu čísla 2 a snáze se používá v matematických výpočtech, ačkoliv skutečná hodnota bude spíše kolem 70).

Pokud se útočník rozhodne vyzkoušet proti Vaší zprávě všechna možná hesla, nazývá se tento postup *útok hrubou silou* (známější je anglický termín *brute-force attack*). Pravděpodobnost jeho úspěchu závisí na množství možných komunikačních hesel, a to je zase závislé na délce komunikačního hesla. Zjednodušeně řečeno, s každým dalším znakem v hesle se obtížnost útoku zvyšuje 64-krát.

Například šestiznakové komunikační heslo nabízí $64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 = 68\,719\,476\,736$ možností. To může vypadat jako velké číslo, ale pokud útočníkům počítač zvládne vyzkoušet milion hesel za sekundu (což současné počítače zvládnou), dostane se k Vašemu heslu nejpozději za 68 719 sekund, což je méně než jeden den.

Avšak dvanáctiznakové heslo nabízí již $64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 \cdot 64 = 4\,722\,366\,482\,869\,645\,213\,696$ možností. Počítač, který by dokázal vyzkoušet milion hesel za sekundu, by potřeboval 149 745 258 **roků** k tomu, aby prošel všechna dvanáctimístná hesla. To je doba, která uplynula od věku dinosaurů.

Dají se vybudovat speciální počítače, které dokáží ověřit mnohem více než milion hesel za sekund, dejme tomu milionu. Ani tyto počítače si však neporadí s opravdu dlouhými hesly.

Jaké jsou tedy vhodné délky komunikačních hesel pro SMS 007? V následující tabulce budeme předpokládat, že hesla jsou volena náhodně, a že na každý znak připadá 64 možností.

Délka hesla	Příklad	Kolik je možných hesel	Poznámka
6 znaků	5aYz1e	68 719 476 736	Nepoužívejte takto krátká hesla ve vážně míněné komunikaci. Heslo této délky odolá Vaší sestře, manželovi nebo sousedům, pokud nejde zrovna o Jamese Bonda. Pro závažnou komunikaci v každém případě volte delší hesla (viz další řádky tabulky).

Délka hesla	Příklad	Kolik je možných hesel	Poznámka
10 znaků	q303cnOS7a	1 152 921 504 606 846 976	<p>Minimální délka hesla pro vážné nasazení, pokud je Vaším protivníkem malá či střední organizace, která nemá dostatek finančních prostředků a technického know-how.</p> <p>Hesla této délky lze zlomit například masivním Internetovým útokem, zahrnujícím miliony počítačů, nebo vybudováním speciálních hardwarových zařízení v cenách kolem milionu dolarů (taková zařízení se neprodávají, musela by se speciálně vyvinout).</p> <p>Použití hesel této délky je akceptovatelné v případě, že tajemství, která chráníte, mají hodnotu menší než zhruba milion dolarů, a nezáleží na nich příliš dlouho.</p> <p>V roce 2015 mohou existovat počítače, které budou lámat 10-znaková hesla stejně snadno jako nynější počítače lámou 6-znaková. Pokud tedy chcete chránit svá tajemství i proti budoucím útočníkům, volte delší než 10-znaková hesla.</p>
15 znaků	kdhU82Bz02rdaIj	1 237 940 039 285 380 274 899 124 224	<p>Bezpečné proti veškerým současným útočníkům, s možnou výjimkou NSA (americká bezpečnostní služba zodpovědná za šifrování a útoky proti němu).</p> <p><i>Používejte minimálně tuto délku hesel,</i> chcete-li být skutečně zabezpečen – například jste-li významným politikem nebo obchodníkem, který zachází s velkými finančními hodnotami.</p> <p>Hesla této délky by měla být bezpečná minimálně na 15 let dopředu.</p>

Délka hesla	Příklad	Kolik je možných hesel	Poznámka
22 znaků	tzl3ianh1s63jndpj1rnm8	5 444 517 870 735 015 415 413 993 718 908 291 383 296	Největší užitečná délka hesla pro SMS 007. Používaná šifra (AES) má 128-bitové klíče a hesla delší než 22 náhodných znaků Vám již nepřidají na bezpečnosti. Použijte heslo této délky, chcete-li dosáhnout maximální bezpečnosti prostřednictvím SMS 007. Hesla této délky by měla být bezpečná proti komukoliv na Zemi a po mnoho let dopředu.

Volba kvalitních komunikačních hesel = Vaše bezpečnost!

- používejte dlouhá náhodná komunikační hesla a řiďte se podle výše uvedených rad při jejich konstrukci,
- nikdy nesdělujte žádné svoje komunikační heslo nikomu jinému, kromě druhé strany příslušné komunikace (která je naopak znát musí),
- pokud možno nepište komunikační hesla na papír. Pokud je to zapotřebí, po použití tento papír spalte,
- jako dodatečné opatření můžete hesla pravidelně obměňovat (například každý měsíc se setkáte se svým partnerem, stanovíte nové heslo a přenastavíte je ve svých instalacích SMS 007).

Úprava kontaktu

Kontakt můžete chtít upravit například tehdy, když dotyčný člověk změní telefonní číslo, nebo když jej chcete zatřídit do jiných skupin, nebo když chcete změnit jeho e-mail, poznámku ... nebo když jste si s ním dohodli nové heslo.

V tom případě zvolte v nabídce seznamu kontaktů „Upravit“. Objeví se obrazovka pro úpravu kontaktu. Upravte údaje (pro zadání nových hesel využijte volbu „Nastavení hesla“).

V případě, že chcete změny uložit, stiskněte „OK“, v případě, že chcete odejít bez uložení změn, stiskněte „Zpět“.

Odeslání zprávy kontaktu nebo skupině

Můžete odesílat zprávy jednotlivým osobám ve svém seznamu kontaktů, nebo celým skupinám. Zprávu začnete tvořit tím, že najedete kurzorem na příslušnou skupinu nebo kontakt, a zvolíte z nabídky „Poslat“. U jednotlivých kontaktů nemusíte ani volit „Poslat“, stačí najet na ně kurzorem a stisknout je (u skupin slouží stisk k jejich otevírání a zavírání).

Informace o psaní a odesílání zpráv najdete v kapitole „Zprávy“

Odeslání kontaktu

Můžete odeslat kontakt ze svého seznamu někomu jinému pomocí SMS. V takovém případě budou odeslány následující údaje: Jméno, Telefon, E-mail a Poznámka. Nebudou odesílána hesla ani žádná další nastavení!

Přejete-li si odeslat kontakt pomocí SMS, zvolte z nabídky „Odeslat kontakt“. Dále se postupuje obdobně jako u odesílání běžné zprávy – viz kapitolu „Zprávy“.

Mazání kontaktu

Kontakt můžete smazat buď ze skupiny, nebo úplně.

V případě, že najedete kurzorem na kontakt ve skupině jiné, než je skupina implicitní (nejvyšší, původní skupina „Vše“), a zvolíte „Smazat“, budete dotázáni, zda skutečně chcete smazat kontakt z této skupiny. V případě, že budete souhlasit, bude kontakt smazán z této skupiny (zůstane ve všech ostatních skupinách).

V případě, že najedete kurzorem na kontakt v implicitní skupině (nejvyšší, původní skupina „Vše“), a zvolíte „Smazat“, budete dotázáni, zda skutečně chcete nevratně smazat kontakt. V případě, že budete souhlasit, bude kontakt smazán úplně – ze všech skupin, které jej obsahovaly.

SMS 007 Manager – rozšiřující schopnosti v seznamu kontaktů

Verze SMS 007 Manager umožňuje v seznamu kontaktů dvě další operace – volání a import kontaktů ze seznamu nacházejícím se v telefonu.

V případě, že si přejete zavolat některému ze svých kontaktů, najedte na něj kurzorem a zvolte z nabídky „Volat“. Pozor, tento hovor nebude nijak chráněn proti odposlechu!

V případě, že si přejete importovat kontakty ze seznamu nacházejícího se v telefonu, zvolte „Přidat z kontaktů“. Můžete být dotázáni na jméno databáze, ze které si přejete kontakty importovat. V takovém případě zvolte databázi.

Následně se objeví seznam kontaktů, které se nacházejí ve Vašem telefonu. Můžete v něm vyhledávat pomocí příkazu Najít, nebo si rovnou vybrat některý ze zobrazených kontaktů. Seznam kontaktů se načítá po nějakou dobu, takže je vhodné vyčkat, než se načte celý. O průběhu načítání budete informováni.

Příkazem „Najít“ můžete v seznamu kontaktů vyhledávat. Zvolíte-li jej, objeví se obrazovka s jedním textovým polem, do něž bude možno zadat hledaný výraz. Vložte jméno nebo jeho část a zvolte „Najít“. Můžete vyhledávat i s použitím diakritiky. Na velikosti písmen nezáleží. Systém vyhledá kontakty odpovídající Vašemu zadání a zobrazí je.

V seznamu kontaktů nacházejícím se v telefonu nyní zvolte ten kontakt, který si přejete přidat do interního seznamu aplikace. Kontakt bude načten a zobrazen. Pokud máte u kontaktu zadáno větší

množství telefonních čísel, budete požádáni, abyste z nich jedno vybrali. Nyní zvolte „Přidat“. Objeví se obrazovka pro přidání kontaktu, v níž budou předvyplněny údaje získané z telefonu. Stačí už jen zadat komunikační heslo.

Zprávy

Těžištěm programu „SMS007“ je odesílání a přijímání SMS zpráv. Odesílané a přijímané zprávy mohou mít nanejvýš 200 znaků a mohou obsahovat libovolnou diakritiku (písmena s háčky a čárkami, ale i polské nosovky atd). Do seznamu zpráv se dostanete z hlavní nabídky aplikace po volbě „Zprávy“.

Po „čerstvé“ instalaci aplikace je seznam prázdný, až na implicitní skupinu „Vše“. Skupinu „Vše“ není možno smazat, ale je možno ji libovolně přejmenovat; bude umístěna vždy nahoře v seznamu zpráv.

O skupinách platí totéž, co o skupinách kontaktů – mohou být otevírány, zavírány, přejmenovávány a mazány. Maximální počet skupin je 60. Jedna zpráva může náležet do libovolného počtu skupin. Jediný rozdíl proti skupinám kontaktů spočívá v ikonách. Otevřená skupina se zprávami je symbolizována obrázkem otevřené zásuvky, zavřená skupina je symbolizována zavřenou zásuvkou.

Výpis zpráv, typy zpráv a jejich barevné označení

Zprávy jsou v seznamu řazeny vzestupně podle času, poslední zpráva tedy bude nejvýše. Ikony zpráv se liší barvou podle toho, v jakém stavu se zpráva nachází

Oranžová – doručená, dosud nepřečtená zpráva.

Modrá – doručená a přečtená zpráva.

Zelená – odeslaná zpráva.

Bílá – uložený koncept zprávy.

Červená – zpráva, jejíž odeslání selhalo, nebo bylo uživatelem zakázáno.

Hromadné mazání

Počínaje vydáním 1.0.4 se v seznamu zpráv nachází příkaz: „Hromadné mazání“. Za pomoci tohoto příkazu můžete kdykoliv pročistit seznam zpráv a ponechat v něm jen poslední 3, 5, 7 nebo 10 zpráv. Stejně jako automatický mazač, ani tento příkaz nemaže archivované zprávy.

Psaní nové zprávy

Začít psát novou zprávu je možno buď ze seznamu kontaktů, nebo ze seznamu zpráv (pod volbou „Nová zpráva“. Objeví se obrazovka, na níž se nachází okénko pro zápis zprávy. Maximální délka zprávy je 200 znaků. V dalším textu budeme tuto obrazovku nazývat „Obrazovkou pro zápis zprávy“.

Nabídka „Obrazovky pro zápis zprávy“ se liší podle toho, zda rozepsaná zpráva má určeného adresáta, nebo nikoliv.

V případě, že zpráva má určeného adresáta, je nabídka následující:

Poslat – zvolte, chcete-li zprávu odeslat (viz podkapitola „Odesílání zprávy“).

Zrušit – zvolte, chcete-li rozepsanou zprávu zahodit (nebude uložena!).

Smazat adresáta – zvolte, chcete-li smazat adresáta.

Uložit – zvolte, chcete-li uložit koncept rozepsané zprávy a ukončit momentální práci (koncept najdete v seznamu zpráv pod označením „bílé obálky“).

Smazat – zvolte, chcete-li odstranit dosud zapsaný text a začít znova.

V případě, že zpráva nemá určeného adresáta, je nabídka následující:

Přidat – chcete-li přidat adresáta (buď ze seznamu kontaktů, nebo nového).

Zrušit – zvolte, chcete-li rozepsanou zprávu zahodit (nebude uložena!).

Uložit – zvolte, chcete-li uložit koncept rozepsané zprávy a ukončit momentální práci (koncept najdete v seznamu zpráv pod označením „bílé obálky“).

Smazat – zvolte, chcete-li odstranit dosud zapsaný text a začít znova.

Povšimněte si, že zprávu bez adresáta není možné odeslat. Než odešlete zprávu, musíte zvolit adresáta – viz podkapitola „Volba adresáta“.

Volba adresáta

V případě, že chcete odeslat zprávu, která dosud nemá určeného adresáta, musíte jí adresáta přiřadit. To se provádí volbou „Přidat“ v rámci „Obrazovky pro zápis zprávy“.

Dostanete na výběr ze dvou možností:

Vybrat ze seznamu – pokud chcete zprávu odeslat nějakému kontaktu nebo skupině kontaktů

Zadat nového – pokud chcete zprávu odeslat někomu, kdo není ve Vašem seznamu kontaktů. V takovém případě musíte vyplnit jeho telefonní číslo v mezinárodním tvaru (+420xxxxxxxxx).

Vyberte jednu ze dvou možností a zvolte „Pokračovat“.

Pokud jste zvolili „Vybrat ze seznamu“, objeví se seznam kontaktů: najedte kurzorem na kontakt nebo skupinu, kterou si přejete, a zvolte opět „Pokračovat“. Dostanete se zpět na „Obrazovku pro zápis zprávy“, nyní však s přiřazeným adresátem.

Pokud jste zvolili „Zadat nového“, provede se kontrola čísla na mezinárodní formát a následně se dostanete ihned zpět na „Obrazovku pro zápis zprávy“, nyní však s přiřazeným adresátem.

Odesílání zprávy

V případě, že jste spokojen se zprávou a zpráva má přiřazeného adresáta, můžete ji odeslat pomocí volby „Poslat“.

Objeví se obrazovka s dotazem, zda chcete odesílanou zprávu šifrovat, a s dotazem „Poslat jako přísně tajnou?“ Možnosti jsou následující:

Ano – odchozí zpráva bude zašifrována. Pokud jde o zprávu skupině, rozdělí se do tolika zpráv, kolik je ve skupině kontaktů, a každá z těchto zpráv bude zašifrována a odeslána zvlášť. Pokud jde o zprávu kontaktu, bude odchozí zpráva zašifrována pomocí jeho hesla. Pokud jde o zprávu neznámé osobě, budete dotázáni na heslo, s jehož pomocí se má zpráva zašifrovat.

Ne – odchozí zpráva nebude zašifrována.

Zpět – vrátit se na „Obrazovku pro zápis zprávy“.

Pokud zaškrtnete „Poslat jako přísně tajnou“, bude zpráva odeslána jako „Přísně tajná“ - viz

podkapitulu „Přísně tajné zprávy“.

Nezašifrované zprávy nemohou být „Přísně tajné“.

Přísně tajné zprávy

Pokud je zpráva označena jako „Přísně tajná“, nebude se ukládat do paměti ani na telefonu odesílatele, ani na telefonu příjemce. Na telefonu odesílatele bude smazána okamžitě poté, co je odeslána.

Na telefonu příjemce bude uložena jen do chvíle, než si ji příjemce přečte. Pak je okamžitě smazána ze všech seznamů.

Příjemce je na tuto skutečnost upozorněn varovným nápisem při čtení zprávy. Viz podkapitola „Čtení zpráv“.

Maximální délka zprávy a počet zpráv

Současná maximální délka zprávy je 200 znaků. Zpráva může být pro účel transportu rozdělena na 1-2 podzprávy, které se platí zvlášť. Odeslání velmi dlouhé zprávy může tedy stát dvojnásobek toho, co odeslání krátké zprávy.

Program „SMS 007“ provádí rozkládání odesílaných zpráv a sestavování příchozích zpráv automaticky, uživatele se to nijak netýká.

Čtení zpráv

Příchozí, odchozí, uložené (atd.) zprávy v seznamu zpráv je možno číst, pokud v rámci seznamu zpráv zvolíte „Upravit“, nebo prostě jen najedete kurzorem na zprávu a stisknete.

Objeví se speciální obrazovka, která shrnuje následující údaje:

- odesílatele/příjemce zprávy, čas
- stav zprávy (Odeslaná, Přijatá ...)
- text zprávy
- použitá šifra
- upozornění na to, zda je zpráva archivovaná
- upozornění na to, zda je zpráva přísně tajná
- zatřídění zprávy do skupin

Tato obrazovka se neobjeví, pokud jde o zprávu zašifrovanou neznámým (neuloženým) klíčem. V takovém případě budete vyzváni, abyste zadali heslo. Zadáte-li správné heslo, zpráva bude rozšifrována a teprve poté se objeví výše zmíněná obrazovka.

Na této obrazovce můžete provést zatřídění zprávy do skupin (následně stiskněte „OK“, aby se změny uložily), nebo můžete zvolit některou z možností nabízených ve Volbách. Tyto možnosti se liší podle typu zprávy, a zahrnují např. následující:

Přeposlat – přepošle zprávu jiné osobě.

Otevřít – otevře uloženou zprávu pro nové úpravy.

Uložit kontakt – v případě, že doručená zpráva obsahuje kontakt, jej uloží.

Poslat znovu – v případě, že odesílání selhalo nebo bylo zrušeno.

Odpovědět – v případě, že jde o příchozí (doručenou) zprávu.

Archivovat – v případě, že jde o nearchivovanou zprávu, lze takto nastavit její archivaci.

Nearchivovat – v případě, že jde o archivovanou zprávu, lze takto zrušit její archivaci.

Uložit číslo – (počínaje verzí 1.0.4) - v případě, že tato zpráva došla z neznámého čísla (tedy z čísla, které dosud nemáte ve svých kontaktech), máte možnost si toto číslo uložit do kontaktů.

Ne všechny možnosti musejí být dostupné naráz, záleží na typu zprávy.

Zatřídění zprávy do skupin

Probíhá zcela obdobně jako zatřídění kontaktu do skupin

Archivace zpráv

Přejete-li si uchránit nějakou zprávu před automatickým mazáním zpráv, nastavte ji jako *archivovanou* (volbou **Archivovat**). Toto své rozhodnutí můžete kdykoliv zrušit volbou **Nearchivovat**.

Nastavení

Pod volbou „Nastavení“ v hlavní nabídce aplikace se nachází podnabídka, která slouží k nastavení vlastností programu. Počet jejích položek je různý podle toho, o jaké vydání systému SMS 007 se jedná.

Heslo aplikace

Zde je možno změnit heslo aplikace. Zadejte do označených políček současné heslo aplikace, a pak dvakrát stejně nové heslo, které musí mít aspoň 8 znaků.

Znalost současného hesla je požadována jako bezpečnostní opatření pro případ, kdyby se neoprávněná osoba dostala ke spuštěné aplikaci.

Zprávy

Zde můžete nastavit automatické promazávání zpráv. Z výroby je automatické promazávání zpráv nastaveno jako zapnuté, s intervalem 1 týden od doručení (vzniku, odeslání) zprávy. Interval je možno nastavit pomocí posuvného jezdce na 1 den, 3 dny, 1 týden, 14 dní a měsíc (30 dní). Pro přenastavení automatického promazávání zvolte patřičné hodnoty a stiskněte „OK“. Nepřejete-li si změnit nastavení, stiskněte „Zpět“.

Automatické promazávání chrání paměť Vašeho telefonu před přeplněním, proto doporučujeme jej nevyplínat. Chcete-li uchránit nějakou zprávu před automatickým promazáváním, nastavte ji raději jako archivovanou (viz kapitola „Zprávy“).

Paměť

Zde nelze v současné verzi nic nastavit, obrazovka slouží pouze jako informativní: kolik je uloženo kontaktů, kolik je uloženo zpráv, kolik místa (v kilobajtech) zabírají a kolik jej teoreticky je ještě volného.

V případě, že se o Vaše zprávy nestará automatické promazávání, měli byste sledovat tuto obrazovku a promazat zprávy ručně, pokud začne jejich počet přerůstat cca 50 (resp. cca 32 kilobajtů - K). Zabráníte tím přeplnění a následnému automatickému smazání paměti.

Pozor, některé telefony (např. Nokia 6230) implementují ukládání do paměti špatně, takže na údaj o tom, kolik teoreticky ještě zbývá volného místa, není spolehlivý. Tuto chybu není možno programátorsky nijak obejít. Spolehlivé jsou pouze údaje o tom, kolik je uloženo kontaktů a zpráv, a kolik místa zabírají.

Start aplikace

Tato položka se nachází jen v některých variantách SMS 007, a to až od vydání 1.0.5. Umožňuje nastavit, zda má aplikace při automatickém startu (když přijde zašifrovaná SMS) přehrát MID a zavibrovat telefonem.

Tato funkce je užitečná zejména na telefonech Nokia série 60 (s operačním systémem Symbian) a série 80 (komunikátory). U těchto telefonů se totiž aplikace při přijetí SMS probouzí „tíše“, takže uživatel neví, že dostal šifrovanou SMS.

Ve verzi SMS 007 Manager se pod položkou **Start aplikace** nachází možnost zvolit zde vlastní melodii přehranou při automatickém startu. Lze přehrávat pouze melodie MIDI kratší než 30 kilobajtů. Melodie jsou načítány z adresáře uvedeného na konci seznamu (například u Nokia Communicatoru jde o adresář Moje soubory/Tóny). Melodie si lze v rámci výběru zkusmo přehrát.

Načítání seznamu melodií z adresáře nějakou chvíli trvá, proto prosím po zobrazení obrazovky

nějakou chvíli vyčkejte.

O aplikaci

Stručná volba, která ukáže jméno, autora a WWW adresu autora aplikace.

Počínaje vydáním 1.0.4 je součástí hlášení „O aplikaci“ i stahovací klíč, s nímž byla aplikace nainstalována. Jde o desetimístný řetězec v závorkách na konci obrazovky.

Ve starších vydáních se tato volba nacházela v rámci hlavní nabídky aplikace.

Nápověda

Tato položka se nachází jen v některých variantách SMS 007, a to až od vydání 1.0.6. Umožňuje nastavit tzv. průběžnou nápovědu.

Na horním okraji obrazovky je prostor pro průběžnou nápovědu k obsahu obrazovky (např. „Toto je hlavní menu aplikace, vyberte z něj.“). Tato nápověda může být užitečná začínajícímu uživateli aplikace.

Pokročilý uživatel si však může přát ji vypnout. V takovém případě se na této obrazovce dá nastavit, aby se běžící nápověda nezobrazovala. Toto nastavení se dá kdykoliv změnit. Je-li jednou provedeno, trvá až do další změny.

Místní nastavení

Tato položka je dostupná až od vydání 1.0.7.

Při vyplňování telefonních čísel dokáže systém SMS 007 automaticky doplňovat mezinárodní předčísli. Od výrobce je přednastaveno předčísli +420 (Česká republika). Přejete-li si změnit toto předčísli na jiné, vyplňte jej zde a zvolte „OK“. Od této chvíle bude systém SMS 007 vyplňovat nově nastavené předčísli.

Poznámky na závěr

Chyby výrobců

Některé telefony obsahují chyby ve firmware, které se mohou projevit jako závady činnosti Java-programů. Například Nokia 7650 nepodporuje korektně http spojení, Nokia 6230 nemá správně implementované ukládání do paměti (RMS). V případě, že je taková chyba vývojářům známa, mohou ji obcházet, avšak není možno ošetřovat všechny chyby ve všech verzích telefonů a všech verzích firmware, neboť mnohé nejsou ani dobře známy/dohledatelné. Jiné sice známy jsou, ale obejít je nelze.

Zavírání aplikace

Je vhodné uzavírat aplikaci pomocí volby „Zavřít“ z hlavní nabídky; „červené tlačítko“ by mělo sloužit buď jen v případě, že se nechcete přihlásit, nebo v případě potíží. Zavírání „červeným tlačítkem“ je radikální a mohlo by zasáhnout do ukládaných dat.

Různé telefony reagují na násilné vypnutí aplikace pomocí červeného tlačítka různě. Zkušenosti s Nokii 6230 a 6230i ukazují, že tyto telefony zvládají násilné vypnutí relativně dobře (i když nikoliv vždy bezchybně!!), u Siemensů série 65 je situace horší, může dojít i k závažné ztrátě dat (včetně hesel).