

Short description and installation guide of CryptoSMS.org

This documentation is version 0.3, released August 2007

It refers to the software version 1.01, released on 26/05/2007

Homepage of the project: www.cryptosms.org

Download address of the program to install: www.cryptosms.org/ota

Sourcecode is at: <http://codecoop.org/projects/CryptoSMS/>

Contact us at interest@cryptosms.org

For Developer, Release and User Support lists, see www.cryptosms.org/lists.html

Feedback is very important so please tell us about your experience, successful or not, with this software on your mobile phone to users@cryptosms.org

This documentation, as well as the user documentation and the technical documentation, can be found at: www.cryptosms.org/docu.html

NOTE: CryptoSMS is an open-source software project, released under the GNU General Public License. Any reference to CryptoSMS in this document means cryptosms.org.

Please note also, that you are using the second release of CryptoSMS, which is a beta release. There are some very interesting features still missing and errors may occur. This software has not yet been widely tested – neither on a lot of phones, countries or networks. Please report every issue that occurs.

Contents:

- 0) License & Warranty
- 1) Introduction CryptoSMS
 - 1.1) How it works
 - 1.2) Public/private keys
 - 1.3) Differences to PGP/GPG
- 2) Installation
 - 2.1) Supported Mobile Phones
 - 2.2) Which Version to download
 - 2.3) The download
 - 2.4) The Installation
 - 2.5.) "Ok to communicate via SMS?"
 - 2.6.) Supported languages
 - 2.7) Troubleshooting

0) License of this Document

This document is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 3.0.

Please see <http://creativecommons.org/licenses/by-nc-sa/3.0/> for further details.

This Documentation in no way guarantees that it fully describes the software cryptosms.org.

Please report errors and missing stuff to interest@cryptosms.org.

1) Introduction CryptoSMS

Cryptosms encrypts and decrypts SMS on your mobile phone. It aims to be as simple as possible and easy to use, even if you have had no experience with encryption tools on your computers such as PGP or GPG so far. We have tried to make the user interfaces as close as possible to the usual SMS handling on mobile phones.

1.1) How it works

Cryptosms uses public / private key concepts. To encrypt a message to someone else, you need the public key of that person. If you don't have their key, CryptoSMS will not allow you to send an SMS to

them. This prevents users from sending SMS in plaintext whilst thinking it was sent encrypted. Only your public key will be send in plaintext.

Once you have received the recipient's key, any SMS to this person will be automatically encrypted and then sent.

Receiving a SMS, that is encrypted to you, is almost the same as receiving a plaintext SMS, as you are not forced to enter a passphrase at that moment. The encrypted message will be automatically decrypted with your private key.

Entering of a passphrase is needed when the program is started or after a time out.

1.2) Public / Private Keys

Public / private key encryption (or asymmetric encryption) offers some advantages over symmetric encryption, where the encryption and decryption process is done with the same key and / or password. The problem with symmetric encryption is that once a third person gets hold of the encryption key, all messages can be decrypted. With public / private keys, it is different. You can distribute your public key anywhere so that anyone may use it to encrypt a message to you. To decrypt the message which is encrypted using your public key, your private key is needed, which is in your possession only. The asymmetric encryption used by CryptoSMS has one disadvantage over most symmetric encryption schemes: it is not built for performance and therefore can take a while. On some phones it can take up to 8 minutes to encrypt a message. While CryptoSMS works on these phones, this makes the usage of CryptoSMS a bit unwieldy. However this issue will not play such a significant role in the future as mobile phones are released with greater processing power.

1.3) Differences to GPG/PGP

While the public / private key scheme is well known for users of PGP or GPG, there are differences between the encryption technologies of CryptoSMS and PGP/GPG, both from the user-point-of-view and from the mathematical point of view.

1: With CryptoSMS you don't need to type in a passphrase for message decryption, messages are automatically decrypted when CryptoSMS receives them. This makes the handling of decryption much easier on the limited interface that mobile phones have (imagine having to type in a strong 12 character passphrase into your mobile everytime you wanted to read a SMS). The passphrase is created by you as part of the configuration process when CryptoSMS is first started on your mobile. After this, the passphrase must be entered whenever the program is opened or a time out after a period of inactivity has occurred. This makes sure that only you can access the messages that are sent and received by CryptoSMS. The passphrase is also used for a second purpose, the encryption of the data in your mobile phone.

2: The algorithm used for the cryptography is completely different to what PGP/GPG uses. CryptoSMS is based on elliptic curve encryption. Using elliptic curves for crypting data results in shorter keys than the ones used in PGP/GPG and results in better performance. Shorter keys are just as suitable for the targeted media SMS, which is limited to 160 characters.

If you want to know more about elliptic curve encryption, see http://en.wikipedia.org/wiki/Elliptic_Curve_Cryptography.

CryptoSMS uses elliptic curves following the ECIES Standard and follows the implementation proposed in 'Guide to elliptic curve encryption' by Hankerson, Menezes, Vanstone, Page 189ff. About ECIES, see: <http://en.wikipedia.org/wiki/ECIES>

CryptoSMS uses elliptic curve encryption from sending to receiving SMS. The first time you decrypt a received SMS, CryptoSMS keeps the SMS encrypted on your phone (unless you delete it), but this time with AES256 symmetric encryption, a cipher widely used and known e.g for harddisk encryption. AES256 is very fast, so reopening of a SMS will be much faster than the first time. Information for AES256 can be found here: <http://en.wikipedia.org/wiki/Aes256>.

2) Installation

2.1) Supported Mobile Phones

The first step is to check whether or not your mobile phone meets the prerequisites of CryptoSMS. You will find a list of tested device at www.cryptosms.org/devices.html. Please note that there are emulators and real devices. As certain devices have only been tested on the emulator, please tell us your experiences with the real device at users@cryptosms.org!

Generally speaking, your phone has a good chance to run the program if it meets the following criteria: Java (J2ME) with CLDC 1.0 or CLDC 1.1 and MIDP 2.0 plus the Wireless Messaging API (wmaapi). You can check this if you look for your device here:

<http://j2mepolish.org/devices/devices-vendor.html>. This is comprehensive list of devices.

If your phone does not meet the criteria but is not listed at www.cryptosms.org/devices.html as not working with CryptoSMS, please try anyway as some mobiles do better than others. And please tell us about your success or failure.

2.2) Which version to download

At this current stage, we have not built different binaries for different models. We plan to do this in the future. Meanwhile, please use the default version, which is located at www.cryptosms.org/ota/

2.3) How to get the program onto your mobile

There are two ways you can install the program on your mobile:

1: via a connection between your phone and the internet with a (wap)-browser

2: via a connection between your local desktop computer and your mobile.

If you have software on your local computer that allows the management of your mobile phone, e.g. "nokia pc suite", and can communicate to your phone with a data cable (usually usb), bluetooth or infrared, then this is a good way to install CryptoSMS. If you can't access your phone via your desktop computer you can still download CryptoSMS directly from the net with the phone's browser. Please note: depending on the vendor of your phone, installation procedures vary a bit. We can not cover all cases here.

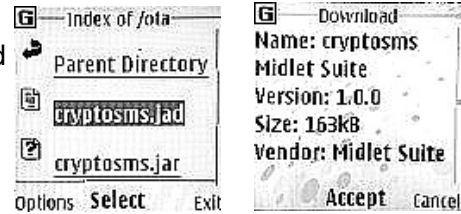
2.3.1.) Downloading via Desktop PC

Download CryptoSMS by starting the browser on your desktop computer and entering www.cryptosms.org/ota/. You will see two files, one called 'CryptoSMS.jad' and one called 'CryptoSMS.jar'. Download the latter to your PC's Desktop or a folder of your choice.

Start your mobile phone management software on your desktop computer and connect your mobile phone in your preferred way. In your phone management software, choose "install application" or the equivalent option. Most applications now show two window panes: one representing the applications folder on your phone and one representing some folder on your desktop computer. In your mobile phone management software, locate the downloaded file in the window representing the pc and transfer it to your phone. This is often done by clicking on an arrow that points towards the window representing your phone or by some entry in the menu of your phone management software. Once you see the file 'CryptoSMS.jar' in the program folder of your phone, you have installed it. For Sony Ericsson devices, the file manager transfers the CryptoSMS jar file to a folder on the mobile. You then need to install the program via your phone.

2.3.2.) Downloading directly to your phone via net

Start the browser on your phone and connect to www.cryptosms.org/ota/ . Here you will see two files, one called 'cryptosms.jar' and one called 'cryptosms.jad'. Click on the latter. A message appears that says something like "OK to install CryptoSMS on your mobile?". Say "Yes" or "OK". Your mobile will start to download the program. This may take a while, but usually not longer than three minutes.



Some phones might allow you to download the cryptosms.jar file without having to download the cryptosms.jad file first. Some might not even support a jad-file, they will only work by downloading the jar-file. However we recommend you try the jad-file first. If problems occur, try downloading the jar-file. See section 2.7 for further information on this topic. (Note: the midlet size and version number might vary from information represented in the picture.)

2.4) The Installation place

The application (called a midlet) will automatically be installed on your phone. But where? This again depends on the type of phone your are using. Some phones will install it to a folder called "Collection", other to the folder "Games" or "Programs". Just look for a program called "CryptoSMS" in any location where other programs such as games or tools like calculators are installed.

2.5.) To trust the program

Depending on your mobile phones settings and also depending on the settings that your telecom provider installed on your mobile, you may be asked questions whether it is OK for CryptoSMS to use the sms messaging functionality. Depending on the trust model, you may have to agree once during installation, or once during setup, or everytime you start it, and / or everytime you want to send an SMS. In some cases, you may give CryptoSMS the right to send and receive SMS by entering the options / more menu while CryptoSMS is highlighted in the folder where it was installed. This makes the usage more convenient as you will not be asked every time before sending an SMS via CryptoSMS.

There are commercial ways to become a trusted party for your mobile phone. However CryptoSMS is not willing to pay the fees to telecom providers and / or manufacturers for this service.

2.6) Supported languages

Cryptosms is designed to offer gui-support in a lot of languages. This means that any language that is encodeable in utf-8 may be supported. This release offers support for:

- English
- Spanish
- Portuguese
- Italian
- German
- French
- Polish
- Turkish

Depending on the language settings in your mobile phone, CryptoSMS tries to use the selected language. If this language is not supported by the program, it uses English as the default.

The languages supported by your phone depend highly on the region you are in, your telecom provider's settings and the manufacturer's settings.

2.7) Troubleshooting

1. "Error downloading file" or any equivalent: check your connection and try again.
2. "Installation failed" or any equivalent: your mobile and CryptoSMS do not work together, possibly because your mobile does not have the required Java capability.
3. "Memory problem" or equivalent: there is not enough memory left on your device. Currently CryptoSMS needs 123kB. In most case, the problem is not the free memory on your phone, but limits for the size of a java application on your phone. In this case, deleting other applications or photos does not help. Please check the maximum allowed midlet size for your phone at the devices list <http://j2mepolish.org/devices/devices-vendor.html> by clicking on your model. Find the entry that tells you about this.
Note, some phones have an ota download limit for jar files and will give you this error message if the size is exceeded. For example, some Nokia phones will only allow a 100kB limit for an ota downloaded jar file. To overcome this problem, you must download the jad file first, the jar file will then download correctly.
4. If your phone is running a version of the windows mobile operating system, you most likely will not (yet) be able to use CryptoSMS. This is because windows mobile is using (as far as we know) a full J2SE virtual machine, not the J2ME java virtual machine. However some windows mobile devices do support J2ME (eg KTC Jasjar) so please check the specifications of your phone. We are planning to release a J2SE compatible version of CryptoSMS. Please show your interest in this version by providing us with information about your phone and its java specifications.

A detailed documentation how to **use** CryptoSMS can be found at www.cryptosms.org/docu.html

~End of Installation documentation~