On-Core Software, LLC.
893 Sycamore Ave.
Tinton Falls, NJ 07724
United States of America

Website: http://www.on-core.com
Technical Support: support@on-core.com
Information: info@on-core.com
Phone: (732) 842-1973
Fax: (732) 842-3234

Documentation revision: March 21, 2011 (v1.4)

TABLE OF CONTENTS

Introduction

Thank you for purchasing On-Core SecuMail. Here at On-Core, we strive to build quality products and would love to have feedback from you on our applications. The following gives you instructions for the program, along with contact information in the event you require technical support.

If you are viewing this document on your iPhone, iPad or iPod Touch, we recommend that you turn your device so it is in landscape mode. Then pinch & expand the view so that the text is stretched to use the entire screen to make this document easier to read. Note that this document can also be download to your computer. Please visit our website http://www.on-core.com/secumail and look for it on the SecuMail page.

Features

- Public Key Encryption and Decryption.
- Symmetric Encryption and Decryption.
- Supports OpenPGP key v4 format.
- Supports the following symmetric algorithms: AES-256, AES-192, AES-128, Blowfish, Cast5, 3DES.
- Option to remember Key pass phrases.
- Server passwords and Key pass phrases are stored in the device key chain, for maximum security.
- Handles gpg, pgp and asc attachments from Mail (for messages and keys)
- Import keys from LDAP, LDAPS, HKP and HTTPS key servers.
- Import keys by Copy/Paste from Safari, Mail or any other program.
- Import keys from pgp, gpg or asc Mail attachments.
- Key Photo ID support.
- Send encrypted text through email or SMS directly from the app.
- Verification of signed messages.
- Ability to sign your messages.

Feedback

We encourage all users to provide us with comments, ideas, or improvements you would like to see in our software. Please do not hesitate to write to: info@on-core.com with any comments, requests, or simply to encourage us to build more great software.

Technical Support

Please email us at: support@on-core.com with any issues. We will contact you as soon as possible to help you resolve any problems. Our technical support line is available Monday through Friday, from 10 AM to 6 PM Eastern Standard Time.

About SecuMail

SecuMail is a partial implementation of the OpenPGP standard (RFC2440,RFC4880) that leverages your current cryptography infrastructure and allows your iOS devices to interoperate with it.

It currently implements a subset of the standard that allows you to encrypt and decrypt OpenPGP messages. It also gives you many options for easily importing and exporting your keys and encrypted messages.

Note: At this time, SecuMail does not support the older version 3 key format.

Overview

SecuMail is divided in four sections: Encrypt, Decrypt, Keys and Settings.

Encrypt allows you to enter or paste text, and then encrypt it by either using a public key or using a symmetric cipher with a pass phrase. The resulting encrypted text can be emailed, SMS or placed on the clipboard.

Decrypt input an encrypted OpenPGP message, and then decrypt it. If the message uses a symmetric cipher, you will be prompted for the pass phrase. If it uses public key cryptography, the necessary key for decryption will be located among your collection of keys, and used to decrypt the message (asking you for a pass phrase in the process, if they key requires it).

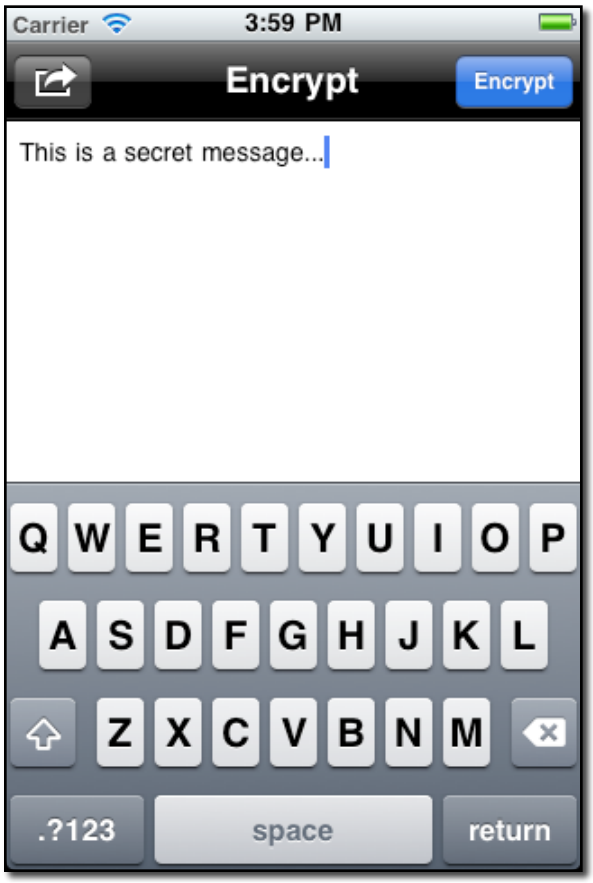
Keys is where you do your key management for public key cryptography. It lists all the keys you've imported that are available for encryption and decryption. It also allows you to add new private or public keys.

Settings allows you to specify default values for some operations and also let's you configure key servers and other program options.

Signing - Signed messages will be verified for authenticity. You can sign your messages when sending.

Below we go into more detail about each section and options. We also discuss integration with other iOS applications.

Encryption



Encryption is done through the Encrypt screen. Simply type in the text to be encrypted. For your convenience, if you already have the text you want encrypt in the clipboard, simply tap the **Action** button on the top left and select **Clear and Paste** or **Clear and Paste Quoted** (if you want SecuMail to automatically quote the text pasted). You can also use the standard paste by double-tapping in the text area. You can also quickly clear all the text by selecting **Clear** from **Action** menu.

Once the text to be encrypted is entered, tap on the **Encrypt** button on the top right of the screen. At this point you will be asked to choose the encryption mode: **Public Key** or **Symmetric**, unless you have specified only one method in the Settings *Mode* option.

Symmetric simply requires you to enter a pass phrase which will be required to decrypt it by any other party. When using Symmetric encryption, you will be prompted to input a pass phrase that will be used to encrypt the message.

Public Key requires that you have a public key for the person for whom you want to encrypt this message. When Public Key is selected, you will then be taken to a screen that will allow you to select the public key(s) to use to encrypt the message. Tap on the row to add that person and a checkmark will appear on the right hand side. You can tap on additional rows to add multiple recipients. When finished, tap on the ***Done*** button.

Note: that if you do not have any keys, you will need to import one before you can use this feature (or use Symmetric encryption instead).

Note: If you only going to use one encryption method, you can configure SecuMail to use only that method for encryption and after that the system will not need to ask you for the encryption mode every time. This can be set from the *Settings -> Mode* option. It can be set to Ask, Public Key or Symmetric.

Once the encryption is complete, you will be asked for the destination of the encrypted text. The options are: **Clipboard**, **Email** and **SMS** (SMS only supported on iOS 4.0 and higher, for devices that support sending SMS).

Clipboard will place the encrypted text on the clipboard. You can then use it by pasting it into any other application.

Email will create a new email and attach the encrypted text as an **asc** file. If the encryption method used was Public Key, then the "To" field will also be auto-completed with the email address of the key used. Note that any addtional text you add to the email will NOT be encrypted. Once you are done, save or send the email.

SMS (If applicable on your device) will create a new SMS message containing the encrypted text. Simply fill in the destination number, and send.

Signing your messages

If you want to automatically Sign your messages, you must select your Private key in Settings -> Signing - Key. (please see Setting section).

Decryption

Decryption is done from the Decrypt screen. Text can either be pasted from the clipboard, or if it is an **asc, pgp or gpg** email attachment, it can be opened in SecuMail by opening the attachment in the Mail app and asking it to open in SecuMail. If the text you want to decrypt is in the clipboard, simply tap the **Action** button on the top left, and select **Clear and Paste**.

Once the text to be decrypted is entered, tap on the **Decrypt** button on the top right of the screen. SecuMail will automatically detect if the message is encrypted in Symmetric mode or Public Key mode.

If the message was encrypted in Symmetric mode, you will be asked to enter the pass phrase to decrypt it. If a Public Key was used to encrypt the message, then SecuMail will try to find the decryption key in your collection of keys. Once it finds the matching key, it will use it to decrypt the message. If the key requires you to enter a pass phrase, then you will be prompted for it.

You can tap on the “S” if you want to Show the passphrase as you are typing it. It will change to an “H”. Tap on the “H”if you then want to hide the passphrase. Tap the “X” to clear.

If you want to *Remember Passphrase*, tap on the **On** button.

Note: In Public Key mode, SecuMail will ask you if you want it to remember your pass phrase for the key that was used to decrypt a message. If you choose to remember the password it will be used automatically when decrypting messages. The period of time that a password can be stored is accessed from *Setup -> Forget Passphrases*. You can have SecuMail 'forget' all the stored pass phrases from the Settings screen by tapping on the *Forget Stored Passphrases Now* button.

Once the message has been decrypted, the resulting decrypted message will appear on the text area of the screen, replacing the encrypted message. You can tap the *Action* button on the top left, and select **Copy and Clear** to copy the text to the clipboard. You can also clear all the text by selecting the **Clear** option.

If a message that was sent to you was Signed by the sender, you will see the line "**Signature Verified Successfully**". If the signature is invalid it will say "**Signature Verification Failed**". To see details about the signing, as shown in this picture, tap on the signature row and the details will pop-up.

Key Management

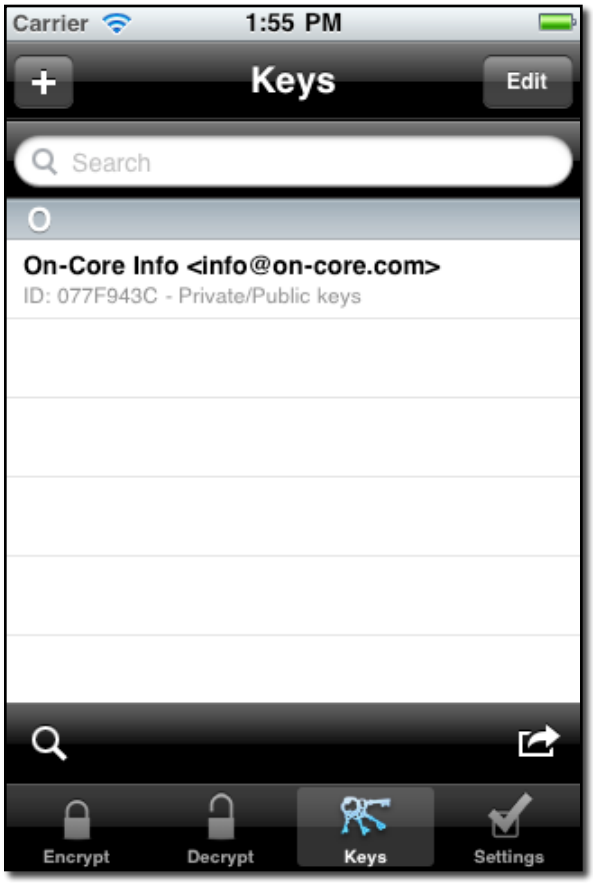
The Keys screen allows you to import and manage your encryption and decryption keys used in Public Key mode.

The search box lets you quickly find the key you are looking for among your collection of keys.

Selecting a key gives you the option to copy the public key (or private key, if available) to the Clipboard, Email or SMS, so you can easily distribute it.

To import a new key to your collection, tap the **+** button on the top left. You will be prompted to import the key **From Clipboard** or **From Key Server**.

From Clipboard will attempt to import a key from the contents of the clipboard. Note that the contents should be armored, OpenPGP-compliant key text. This option gives you the convenience of importing keys by copy and pasting them from other apps, such as Safari or Mail.



Note: If you're concerned about sending the keys temporarily over email, this is what you can do:

- Export one or more keys into an **asc** file.
- Rename the file as “keys.txt”.
- Encrypt the file with a **symmetric** cipher.
- Email the encrypted file.
- Open the attachment in the Mail app, then tap on the attachment to open in Secumail. It will prompt for the passphrase to decrypt.
- Once decrypted, use the action menu on the top right to copy the entire **asc** message to the clipboard.
- Now go into the Keys tab, and tap on the Add (**+**) button, and select "From Clipboard".
- Your keys should now be imported.

From Key Server will allow you to search and import keys from a key server. Note that in order to use this option, you need to have at least one key server configured. You can configure key servers from the Settings screen (please refer to the Settings section for instructions).

You can also email keys to your device and open them in an Email if they have the .asc, .pgp or .gpg extension. If you tap-n-hold on the attachment you can then Open with SecuMail.

To delete keys

Tap on the **Edit** button on the top right. Next, tap on the red circle on the left side of the key you want to delete, and then tap the **Delete** button when it appears. You can also swipe across the key to bring up the **Delete** button.

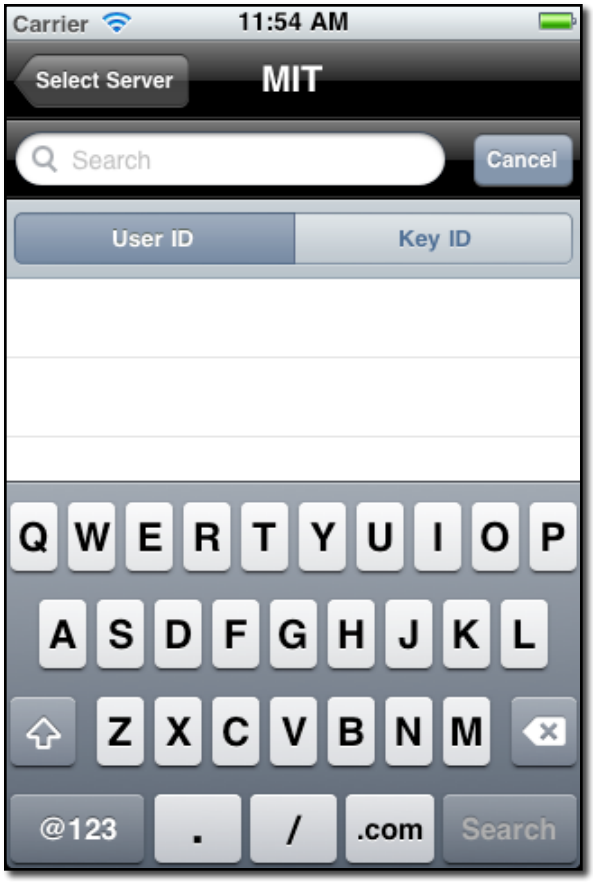
To Export Keys

The action button on the bottom right, allows you to batch **Export All Keys** (public and private) or **Export All Public Keys** (public keys only). You can either export them to the Clipboard or to send them via an Email.

(continued on next page)

Importing Keys from a Key Server

When you have more than one key server configured, you will be asked to select the key server from which you want to import keys. If you only have one key server configured, you will be taken to the server screen directly.



You can search for keys based on **User ID** or **Key ID**.

User ID is the most common way to search for keys and normally includes a name and email address. The search is performed using wildcards, so you don't need to know the exact **User ID**.
Enter the search criteria and then tap **Search** on the virtual keyboard to begin the search.

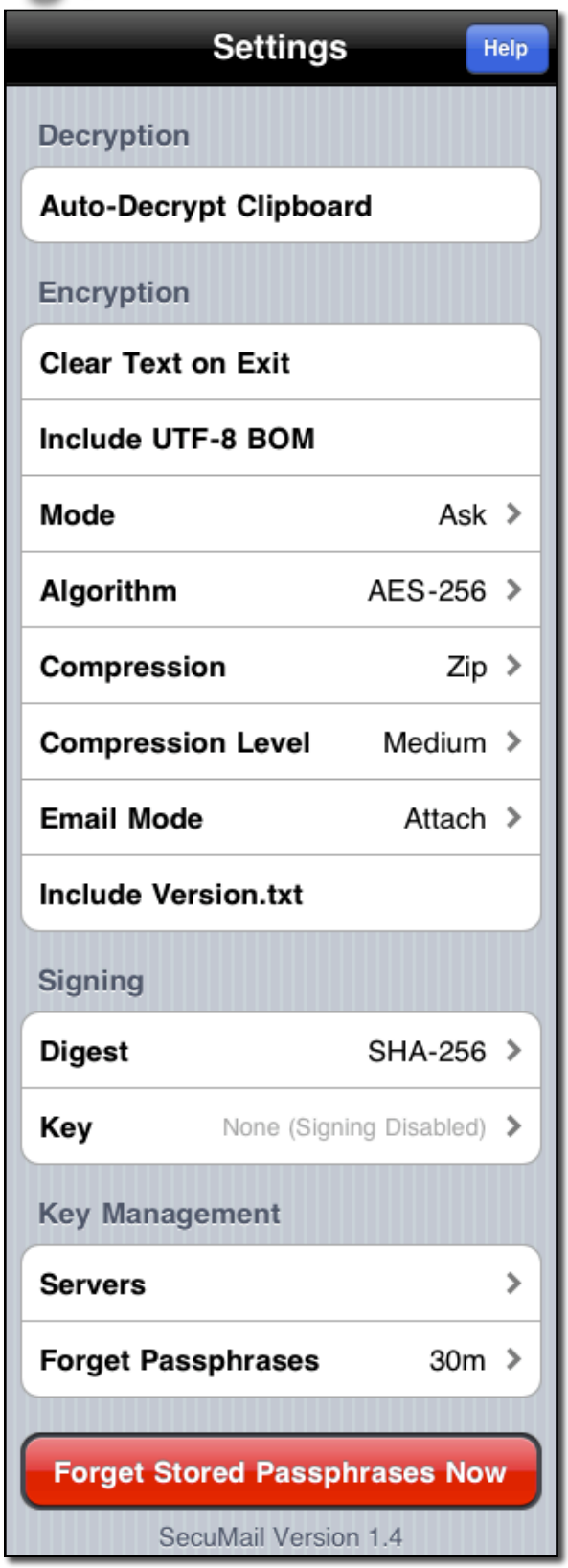
If you already have a **Key ID** you are looking for, just tap the **Key ID** scope button, then enter your **Key ID** in the search field. The search for **Key ID** is exact, so make sure you entered the **Key ID** correctly. While some programs require you to enter a 0x prefix before the **Key ID**, this is optional in SecuMail. Tap **Search** on the virtual keyboard to begin the search.

Different servers will return a different number of search results. Some of them will require you to be more specific by telling you there were too many results for your query. If that's the case, please try to be more specific in your search criteria and try the search again.

Once you have found the key you want to import, tap on it. It will be retrieved from the key server and you will be asked to confirm the import operation. After the import is complete the newly imported key will appear on your list of available keys. If the key can be used for Public Key encryption or decryption, it will now be available for those operations.

Settings

SecuMail can be configured and customized through the Settings screen.



Decryption Settings

If you want SecuMail to automatically decrypt a PGP message that is in the Clipboard when SecuMail is launched, tap on the **Auto-Decrypt Clipboard** row and a *checkmark* will appear on the line.

Encryption Settings

Clear Text on Exit If you want SecuMail to automatically clear the Encrypt window's text when you exit SecuMail, tap on **Clear Text on Exit** and a *checkmark* will appear on the row. The benefit of this is that you will not have to worry about any unencrypted text in the app if someone else picks up your device. The disadvantage is if you need to launch another app and then come back, your text will be cleared.

Include UTF-8 BOM Check to include an UTF-8 Byte Order Mark (BOM) prepending the text to be encrypted. Some text editors require this mark in order to automatically identify the text encoding.

Mode allows you to set a specific encryption mode. If you set it to Ask (the default), SecuMail will ask you what mode do you want to use every time you encrypt information. If you set it to Public Key or Symmetric, SecuMail will automatically use that mode when encrypting information.

Algorithm lets you define which encryption algorithm to use when encrypting in Symmetric mode.

Compression lets you set the way that the PGP message can be compressed. You can choose between: None, Zip (default), ZLib or BZip2.

Compression Level If a compression is set, you can specify the level to which the data is compressed. Low gives less compression, but processes faster. The default is Medium. High will give you the best compression, but will take longer to process.

Email Mode The Email Mode will let you select how the encrypted message will be included in your email.

- **Attach** - The encrypted message will be attached in a file with the ".asc" extension.
- **Body** - The encrypted message will be placed in the body of the email.
- **Attach & Body** - The encrypted message will be both placed in the body of the email and also attached on a file with the ".asc" extension.

Include Version.txt This option is only available when the Email Mode is set to 'Attach' or 'Attach & Body'. Check this option to include an extra attachment named "Version.txt", which increases compatibility with certain third party programs that specifically look for such attachment.

Signing

If you want to "sign" your messages, you will select the Digest method and choose the Private Key with which you want to sign the messages. You will be prompted for the Passphrase when signing. It can be remembered just like the decryption Passphrase.

Digest is the hashing algorithm used as part of the signing process. The default is SHA-256. The options are: MD5, RIPEMD160, SHA1, SHA-256, SHA-384 and SHA-512.

Key is the Private key that you want to use for signing the messages. Tap on this row to bring up the selection of Private keys. If a key is chosen and you want to discontinue signing messages, just tap on the *Clear* button to clear out the Key.

Key Management

The **Key Management** section lets you configure key servers through the **Servers** option (see next section on how to configure key servers). You can also set how long will SecuMail will remember stored passphrases, by using the **Forget Passphrases** option.

You can have SecuMail remember the passphrase for: Never, 5, 10, 15, 30 or 60 minutes.

If you want SecuMail to forget all stored passphrase immediately, simply tap the **Forget Stored Passphrases Now** button. This will clear the passphrase for Decryption and Signing.

This screen contains the version number of the application. You can tap the **Help** button on the top right to access this documentation from within the app.

Configuring Key Servers

From the Settings screen, tap on the **Servers** row to access the key server list screen.

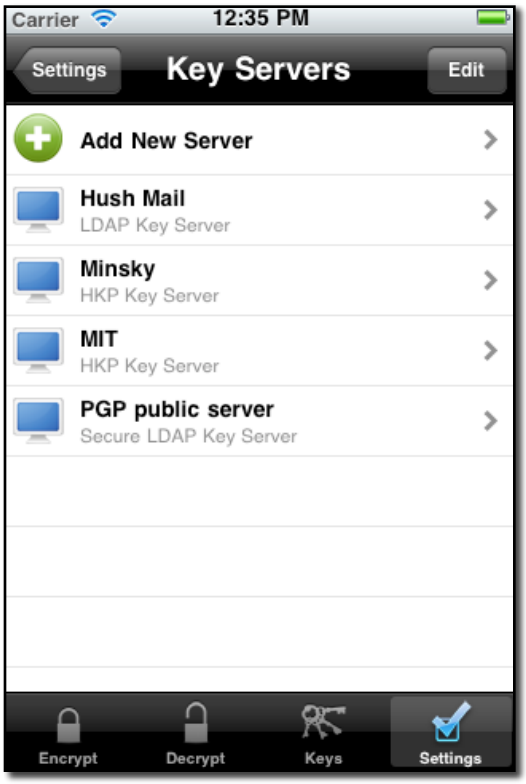
To add a new key server, tap on the **Add New Server** option. That will take you to a new screen that will allow you to enter your key server information.

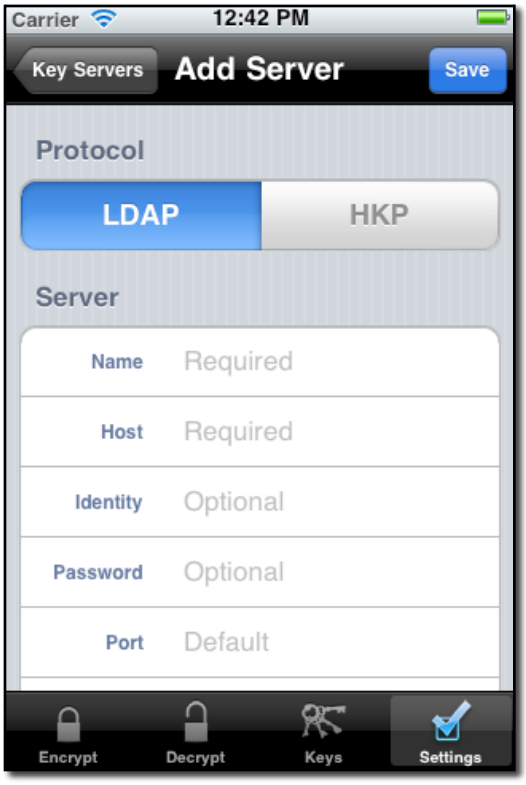
To **edit** key server information, simply tap on the key server you want to edit, and you will be taken to a screen where you can edit the server information.

To delete a key server, tap on the **Edit** button on the top right. Next, tap on the red circle on the left side of the server you want to delete, and then tap the **Delete** button when it appears.
SecuMail supports the following protocols (default port numbers appear in parenthesis): LDAP (389), LDAPS(636), HKP(11371), HTTPS (443).

To use HTTPS, select HKP as your protocol, and make sure the **Use SSL** option is ON.

SecuMail will verify the connection to the server after you tap on the **Save** button on the top right. In the event the verification fails, please double check that all the information provided is correct.





Credits

Portions of this product are: