R10Cipher 5

Key Management

Standard Key Management

Introduction

Key Management is an extremely useful and important part of encryption, yet is often sadly neglected by the developers of encryption software.

In this document the term 'Key' relates to the database record for an individual which contains the following information:

Name
Email Address
Shared Secret
Master Password
Usage Password

If you have several contacts who you communicate with using encryption, how do you keep track of, remember and retrieve the individual Shared Secrets ? **The Key Management database makes this possible.**

Note: Storing information of this nature in a database would under normal circumstances be a security risk in itself, R10Cipher however stores this information in an Encrypted format using 384 Bit encryption and a 56 Character Secret.

By inputting (or importing - see next section) your contacts into the Key Management Database you can retrieve their Shared Secrets and Email Addresses when you need them, quickly and easily.

There are two password fields in the Key Management Database Record. If there is only one person using your Key Management Database then you need only bother with the Master Password, if someone else is allowed to use your Key Management database then they will be given the 'Usage Password' which will allow them to Encode and Decode communications from the contact, but not change any details, including the Shared Secret.

Key Management Record - Passwords			
(Each Key Record is Individually Protected)			
		Master Password	Usage Password
Decrypt Text and Files		*	*
Encrypt Text and Files		*	*
Decode (View) the Key Management Record		*	
Edit Key Management Record		*	
Delete Key Management Record		*	

Shared Secrets and Passwords: Glossary and Usage

Shared Secret

This is the code or phrase that is used to secure a communication between yourself and a particular third party, ie: your client or contact.

Master Password

This is the password that only you should know. It safe guards your Key Management Database records. You could use a different Master Password for each record if you preferred or use a different one for each type of contact, or use the same one for each record. It's entirely up to you, but bear in mind that you have to remember this one ...

Usage Password

Only needed if another individual may be using your R10Cipher to communicate with your contacts. They can retrieve the Shared Secrets for use but cannot see them or change them.

Notes

It is recommended that for each client/contact you assign a different Shared Secret. Make it at least 9 characters, 16 or more is ideal, it doesn't have to be particularly memorable as the Key Management makes it easy for this to be retrieved when needed.

You should secure your Key Management Database and the Shared Secrets using a Master Password. This Master Password should be more memorable as this is the what you will have to enter in order to edit, delete or retrieve the Shared Secrets. I recommend you base this password on a something familiar, for example the first letter of the words of the first two lines of your favourite song. Mix this using upper and lowercase and substitute numbers where possible.

Note: The reason for having a password secure the Shared Secrets is that the Shared Secret is used to encrypt the communication, this communication will be 'in the wild' when transferred over the internet between email or web servers, hence it needs to be unique and strong. Your Key Management Database however is not exposed to the outside world so a small amount of passwords or a single password should be sufficient to encrypt and control access to the records in the Key Management Database.

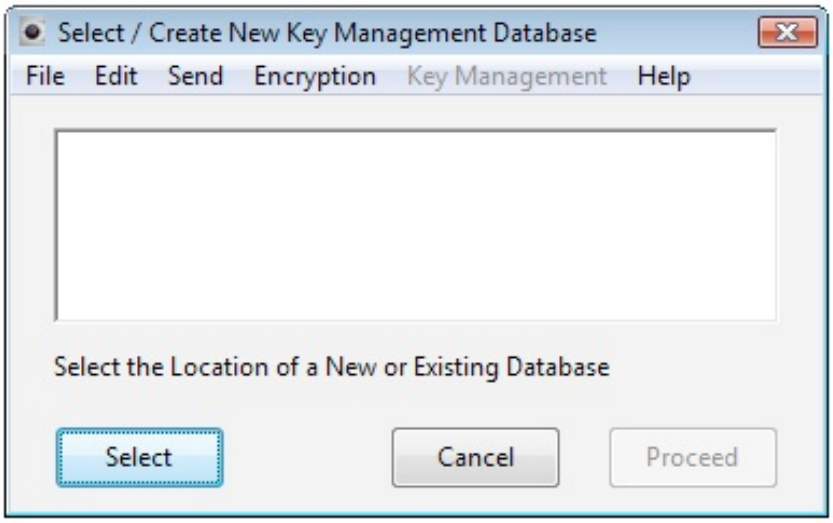
Creating the Key Management Database

Before you can use the Key Management facilities of R10Cipher you need to create the Key Management Database.

This is done by using the Menu Option:

Key Management
Database

You will see the following screen (Windows Vista Version Shown):



Use the Select button to choose a location to store the Key Management Database. You do not have to specify a file name, just a location. The file is named automatically. Once selected the path will be shown. Click Proceed to Save this information.

In future this Key Management Database will be opened automatically, unless you re-visit this screen and choose a different Key Management Database.

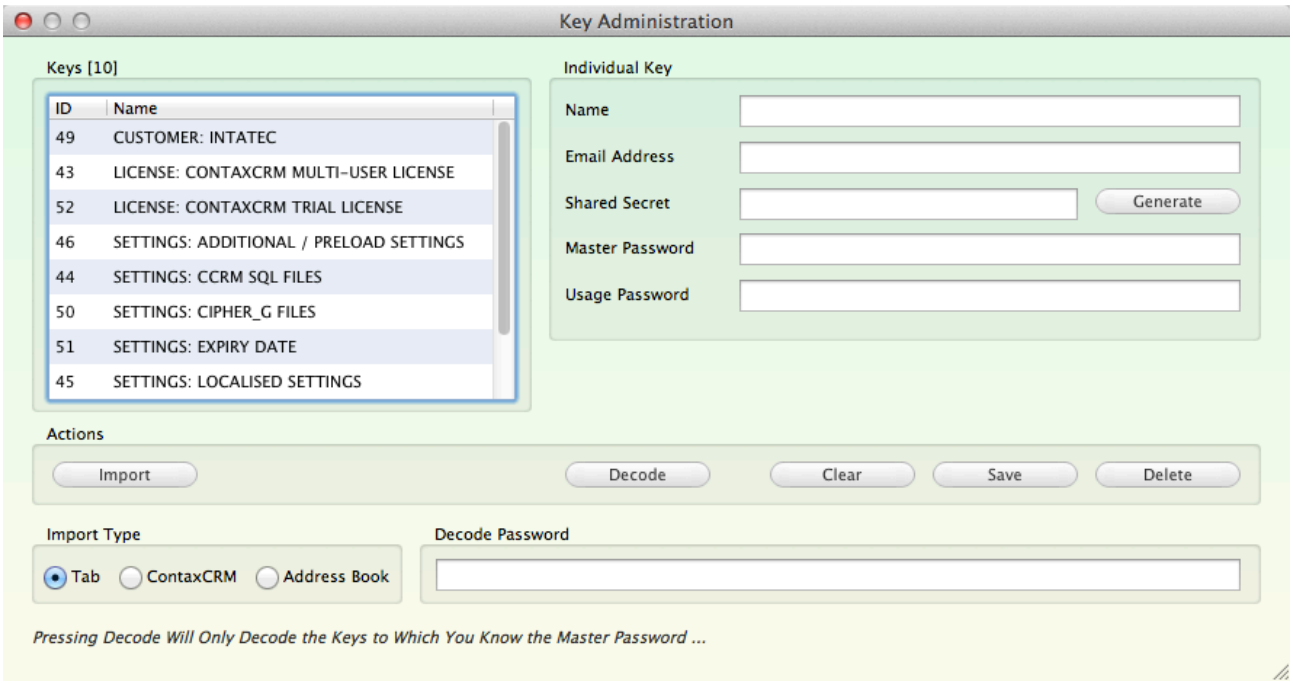
You can choose to save the database in a synchronised folder, such as DropBox, so that your database is available for you even when working remotely.

Key Creation and Administration

The creation of keys is done by selecting the following Menu Option:

Key Management
Administration

You will see the following screen (Mac OSX version shown):



This is where you setup your clients/contacts and your/their Shared Secrets. In addition, for each client you setup you can assign two passwords, a Master password and a Usage Password. *For an explanation of the two passwords see the Key Management Introduction section.*

To **Insert** a contact, just start typing and fill in the five information fields, from Name to Usage Password. When complete press Save, and Save again to confirm.

To **Edit** a contact, select the contact from the list on the left hand side of the screen. You will see the Name and Email Address but the Shared Secret and the Passwords are encrypted and not readable. To view this data and edit it you need to input the Master Password **for this contact** into the Decode Password area of the screen and press the Decode button. You can then edit the information and save it using the Save button.

To **Delete** a contact, select the contact from the list on the left hand side of the screen. You will need to input the Master Password **for this contact** into the Decode Password area of the screen and press the Decode button. You can then press the Delete button to erase the record.

Deleted records are gone and cannot be retrieved.

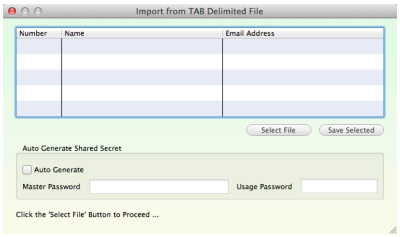
If you intend entering a number of clients or contacts you may already have them stored in a database or spreadsheet somewhere. If that is the case then you should Import the records which will save you time and increase information accuracy.

You will need to edit each record later to apply the Shared Secret and Password(s).

To Import records you have three choices which can be selected using the 'radio' buttons on the bottom left of the window. When you have selected the type of import you require press the Import button. The three choices are:

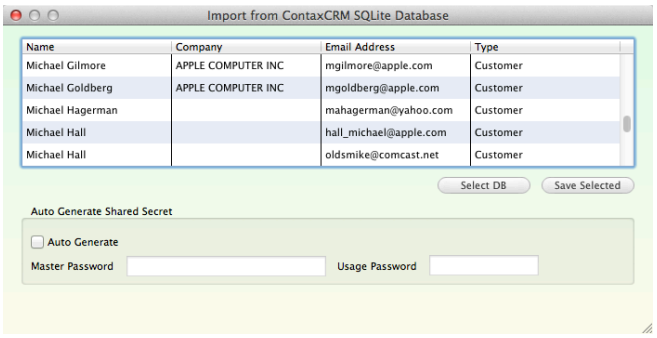
Tab - Tab Delimited

This is the Tab Import Window. The fields required are Name and Email Address. Select the import file using the Select File button. Select the records you would like to import, and save them to the Key Management database using the Save Selected button.



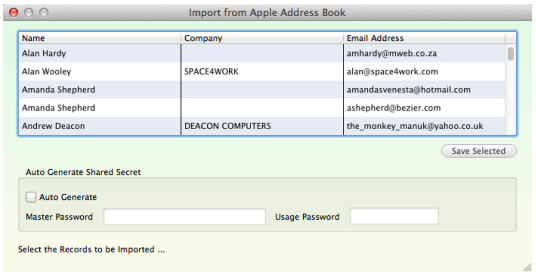
ContaxCRM - ContaxCRM Import

This is the ContaxCRM Import Window. You point R10Cipher at your ContaxCRM database, using the Select DB button, and this pulls data into the import window, allows you to sort by Type and then import the selected records using the Save Selected button.



Address Book - Apple Only

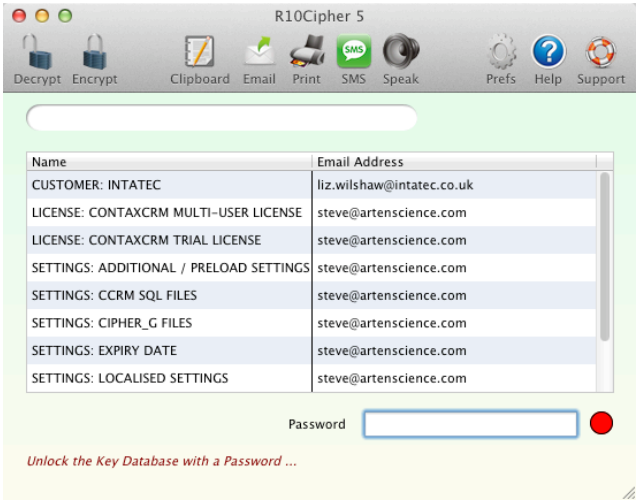
This is the Apple Address Book Import Window. Select the records to import and save them to R10Cipher using the Save Selected button.



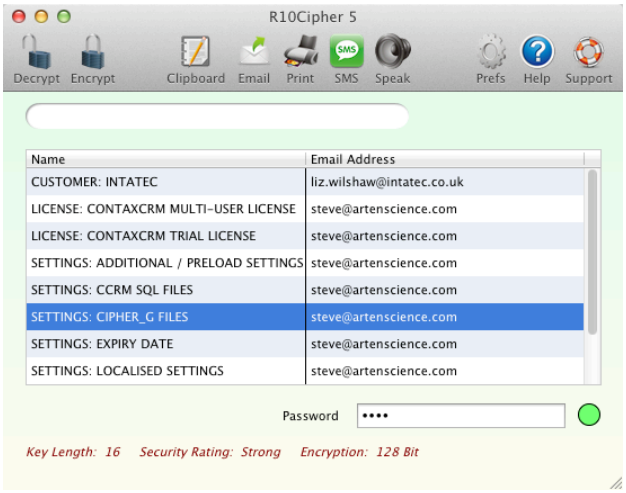
Key Retrieval

Scenario 1: Encrypting or Decrypting Text or a File from within R10Cipher

In these circumstances instead of having to remember and enter the Shared Secret for the contact you can instead go to the **View Menu > Keys** and input the Master or Usage Password for the appropriate contact. Then choose the contact from the list. You can search for the contact and filter the list using the search box on the top right of the screen.



Select the contact in the list. If you have entered the correct Password the indicator will change from red to Green and the Shared Secret fields will be populated.



You can now encrypt text or files without having to enter the Shared Secret.

Another Advantage of retrieving the Shared Secret from the Key Management Database is that if you are sending an encrypted email, R10Cipher will know the email address and fill in the email header appropriately.

So instead of having to remember lots of Shared Secrets and Email Addresses, you only, using the Key Management Database, have to remember a single Password.

Scenario 2: Double Clicking an Encrypted File to Decrypt

When double clicking an encrypted file you now see the following screen:

In these circumstances instead of having to remember and enter the Shared Secret for the contact you can instead input the Master or Usage Password for the appropriate contact.

You can search for the contact and filter the list using the search box on the top right of the screen.

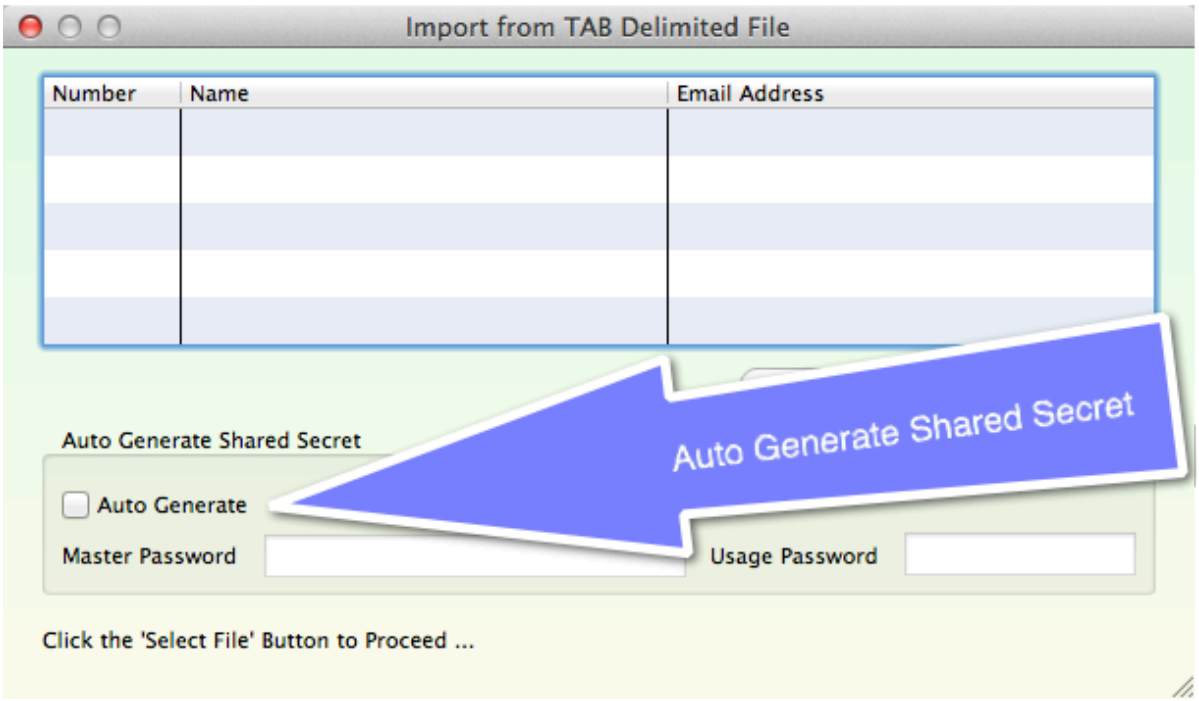
Select the contact in the list. If you have entered the correct Password the indicator will change from red to Green and the Shared Secret fields will be populated.

Click Continue to Decrypt your file.

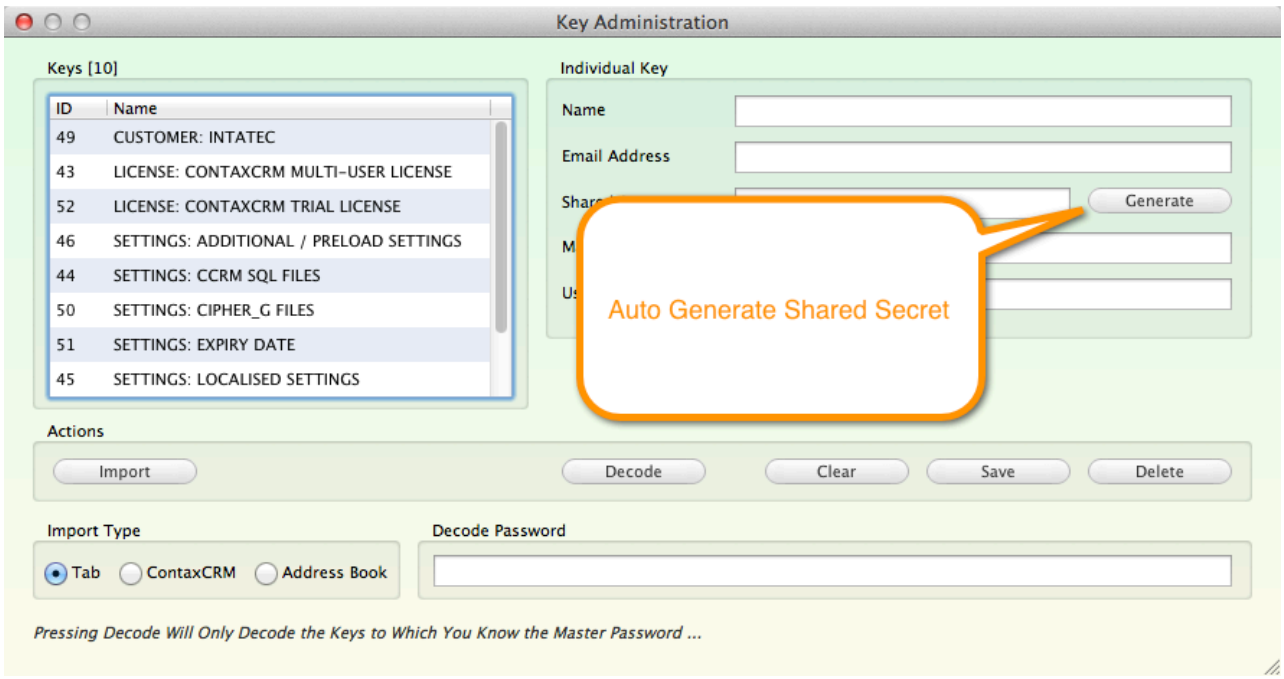
Auto Generate Shared Secrets

R10Cipher from Version 3.1.0 will if you require, automatically generate the Shared Secrets. You of course still need to tell R10Cipher the Master and Usage passwords or else you cannot see the automatically generated passwords in order to inform your clients / contacts of them.

Auto generation can happen during import ...



... or can be done on an individual Key by clicking the ‘Generate’ button.



Distributed Key Management

Introduction

Standard Key Management works very well within a family or small workplace environment. Where it falls over is the large enterprise, corporate or campus scenario. Typically an extra layer is added - the IT Department (queue music from the Jaws film :-)) - their role will likely be to try and ensure consistent use of Shared Secrets throughout an organisation encompassing dozens, hundreds or even thousands of users.

R10Cipher_G

R10Cipher_G is a utility program available separately and at extra cost that allows you to use R10Cipher within your organisation, company, university, lab, or school and manage the Encryption Key Database from a central location. Keep dozens or hundreds of copies of R10Cipher synced across multiple users and multiple sites.

Imagine you have fifty people who you wish to communicate with securely. To ensure security each of their Shared Secrets should be different. Any Shared Secret worth using cannot be remembered easily, not along with forty nine others ! The in-build R10Cipher Key Management database copes with this scenario easily, allowing you to use one Master Password in order to retrieve any of the fifty individual Shared Secrets.

So the next stage is this: What if you and fifty, or even five hundred of your best friends / colleagues need to communicate securely with each other as well as a client base of several thousand ? This is where you need the Centralised Key Management Database Utility, which is an optional purchase.

The Centralised Key Management Database Utility (known as GOD-Mode or G-Mode during development - try saying or typing Centralised Key Management Database utility a few times ...) is launched and pointed at an R10Cipher database nominated as a Master Key Database, ie: one setup and managed by the Company / Department or Individual responsible for your secure communications. G-Mode then populates a MySQL Database with the contents of the Master Key Database, and a text file is edited and incremented, for example from 5 to 6.

The next time any of the users who have had their R10Cipher software configured for G-Mode, load R10Cipher, R10Cipher compares the local database version number with the remote database version number and if necessary syncronises it's local database with the remote MySQL Key Management database.

The syncronisation is one way only, ensuring that the individuals Key Database is reset as per the nominated Master Key Database. It's simple, easy to setup, slick and fast. R10Cipher can now scale very easily in a controlled fashion, with the benefit and added security of distributed and easily backed up information.

You can also setup R10Cipher with your own personal Key Management Database as well which is not designated to sync with the remote database. Perfect for keeping the Shared Secrets for your personal contacts.

The person is control of the Centralised Key Database determines when the syncronisation occurs. A text file named R10Cipher_KMD_Version.r10 should be located in a centralised remote folder (and pointed to from within the R10Cipher Preferences window). This file contains the version number of the database. When you wish your users to get the latest database contents, advance this number appropriately. The next time the users login, syncronisation will occur.

Setting Up R10Cipher_G

This movie shows you how to setup your Centralised Key Database on a MySQL Server.
http://www.artenscience.com/movies/R10Cipher/R10Cipher_G_Setup/index.html

Contact stevecholerton@me.com for Pricing, Availability and Further Information on R10Cipher_G and Distributed Key Management.

###