Title:	Why R10Cipher ?
Author:	Steven Cholerton
Date:	October 2009
Updated:	September 2012
Version:	1.4

Arten Science Limited. Denby House. Loscoe. Derbyshire. DE75 7TA
web: www.artenscience.com email: info@artenscience.com

Arten Science, providing Quality and Innovative Business Solutions

Introduction

This document discusses why you should use R10Cipher to ensure your communications are kept private and confidential.

In this document there is very little discussion of the technology. There is a very good reason for this:

Technology is the straightforward part of security. The real issue that needs addressing is how to make the technology easy and simple enough so that it is used.

Security and encryption are as much about people and processes as technology. What good is security technology if people cannot or will not use it.

R10Cipher was designed from the ground up to be useable by ordinary people. The design for versions 2 through 5 was based almost entirely on feedback from existing and potential future customers.

Overview

R10Cipher is a simple and easy way to safely encrypt your email, text and document files. It is like your documents and email are escorted by a SWAT Team rather than written on a postcard.

R10Cipher offers secure, peer to peer end to end encryption using up to 384 Bit Blowfish encryption.

The encryption technology used by R10Cipher was developed in the UK. Blowfish is a keyed symmetric block cipher which was invented by 'Security Guru' and renowned author, Bruce Schneier, Chief Security Technical Officer at British Telecom, in 1993. It provides excellent encryption and will continue to do so for the foreseeable future. Blowfish is free of patents, and back doors, and Bruce has placed Blowfish in the public domain.

Text and Document Security

It seems that despite the publicity given to security, encryption and identity theft, very few people actually take these threats seriously. Our own government and Civil Service have time and time again been caught out and been exposed as not taking security, our security, even *national security*, seriously.

This is, I sincerely hope, down to individuals being confused about or choosing to ignore security policies and not down to the fact that these organisations don't have any security policies in place.

The reason, I believe, that security is often ignored is because it is perceived as too complicated for the average person. In a lot of cases it is. Security and Encryption are, and need to be, *Complex* - but Not *Complicated*.

If an encryption product could be copied onto your computer, whether it be running Windows, Mac or Linux, if this product could be run from a USB drive or a CD-ROM, if this product was only a few Mb in size and was fast and easy to use requiring no installation, or runtimes, or frameworks, would people be more comfortable using it ?

If you could communicate using this encryption product and the recipient if not already possessing the product, could download it in seconds and use it to decrypt the message without any payment or registration, would people use it ?

If you could encrypt a bunch of files just by dragging and dropping them, could it be any easier ?

If an individual receiving an encrypted document could double click the encrypted document, enter their Shared Secret and have the encrypted document be decrypted and automatically saved to their Desktop under it's original file name, isn't that easy and straightforward enough ?

R10Cipher can do all the above, and more.

An American school teacher recently purchased R10Cipher and now uses it to send messages to the parents of her students. As the 'decrypt only' version of R10Cipher is free of charge, this was done at no cost to the parents and only a few dollars to the teacher. Price along with flexible and fair licensing are additional ways in which R10Cipher triumphs over it's competitors.

Email Security

Some encryption solutions available are in my opinion potentially dangerous, as they give the illusion of security while in the real world being subject to being compromised all too easily. There are a number of common ‘server based’ or ‘black box’ type email encryption systems. These systems encrypt the email whilst in transit.

This is fine as far as it goes, however what about if the email gets sent to the wrong person accidentally ? or if it then gets forwarded accidentally by the recipient ? What about if the recipient’s computer is insecure and her email inbox is reviewed by someone when she is out of the office ?

In my opinion for an email to be considered secure it should be encrypted in such a way that the only people who can view the contents are the sender and the *intended* recipient(s).

R10Cipher is the obvious choice.

Cross Platform

R10Cipher runs on all the modern Operating Systems.

Macintosh OSX

Microsoft Windows

Linux

R10Cipher loves all Operating Systems equally :-)

Communicating Securely In Public

Another area in which R10Cipher can be used successfully is when communication needs to be made between individuals using technologies that are publicly readable. An example would be a blog being written by a world traveller in which he updates his audience daily as to his location and his adventures.

Tagged on the end of a blog post could be an encrypted message that can be decoded only by his wife in which he tells her how much he misses her and can she send him some toilet roll as this item appears to be in short supply in Outer Mongolia.

R10Cipher is ideal for this purpose.

Key Management

One of the problems that was discovered during real world usage of version 2.x was the problem of Key Management. For security purposes, I as an IFA for example, should use a different Shared Secret for each client but how do I remember each of those and who they belong to ? The answer came with version 3 of R10Cipher and the inbuilt Key Management capability.

R10Cipher Version 3 and above features an encrypted database of contact names and their email addresses. Stored against each of these individual records is also their Shared Secret. All of this information can be recalled and used by entering a single master password. I need only my master password to communicate securely with any of my contacts, using their own individual Shared Secrets.

There is also the option of setting a secondary password called a 'Usage Password'. This password allows an individual, maybe a member of staff, to send and receive encrypted communications with the client without ever seeing or having the ability to change that clients Shared Secret.

I believe this method of communicating between large groups of people securely has simplicity and security advantages to the Public Key methods available, whether centralised using a Certificate Authority or decentralised 'Web of Trust' PGP type methods.

Another advantage of R10Cipher in this scenario is that you have the control, you are not relying on a third party, or a web service to handle the encryption.

With R10Cipher it is all done locally.

Summary

Data Security and Privacy are an ideal, a holy grail that we as citizens in the 21st century are striving for. What was once considered a right, is now considered difficult and virtually unattainable.

Convenience and Security are generally seen as being divided by a large gap. Veer to the left of that gap and we have greater Convenience, at the expense of Security. Veer to the right and we have greater Security, at the expense of Convenience.

I don't think it has to be that way. R10Cipher is designed to make security of email, text and documents convenient and easy to use without compromising on security.

Additionally I am using the R10Cipher engine in a number of my products to give inbuilt encryption by default, there is no reason that the data stored within your CRM System or your Reference Manager should be stored as clear text. Built in encryption in all kinds of products is the way forward.

http://www.contaxcrm.com
http://www.myvault4safedata.com

I am also working with other companies who are using the R10Cipher encryption libraries to build encryption into their own products.

Choosing R10Cipher should not stop you using other complimentary encryption systems.

Full disk encryption products such as TrueCrypt add to your overall security and as such work well with R10Cipher. Security is better viewed as a layered approach, there is no silver bullet or one stop shop.

I believe that generally speaking security is looked upon by the man in the street as too complicated and too expensive and as such often gets ignored.

With R10Cipher I hope to change peoples minds and therefore help them protect their own privacy.