

**Mike McBride**





# Contents

<b>1</b>	<b>Encryption Configuration</b>	<b>4</b>
1.1	Introduction . . . . .	4
1.2	Use . . . . .	4
1.3	The SSL Tab . . . . .	4
1.4	The OpenSSL Tab . . . . .	5
1.5	The Your Certificates Tab . . . . .	5
1.6	The Authentication Tab . . . . .	5
1.7	The Peer SSL Certificates Tab . . . . .	5

# 1 Encryption Configuration

## 1.1 Introduction

Many applications within KDE are capable of exchanging information using encrypted files and/or network transmissions.

## 1.2 Use

### WARNING

All encryption schemes are only as strong as their weakest link. In general, unless you have some previous training/knowledge, it is better to leave this module unchanged.

The options within this module can be divided into two groups:

Two options along the bottom of the module, Warn on entering SSL Mode and Warn on leaving SSL mode, allow you to determine if KDE should inform you when you enter or leave SSL encryption.

The remainder of the options are about determining which encryption methods to use, and which should not be used. Once you have selected the appropriate encryption protocols, simply click Apply to commit your changes.

### TIP

Only make changes to this module if specific information about the strength or weakness of a particular encryption method is given to you from a *reliable source*.

## 1.3 The SSL Tab

The first option is Enable TLS support if supported by the server. TLS is Transport Layer Security, and is the newest version of SSL. It integrates better than SSL with other protocols, and it has replaced SSL in protocols such as POP3 and SMTP.

Then next options are Enable SSL v2 and Enable SSL v3. These are the second and third revision of the SSL protocol, and it is normal to enable both.

There are several different *Ciphers* available, and you can enable these separately in the lists labeled SSL v2 Ciphers to Use and SSL v3 Ciphers to Use. The actual protocol to use is negotiated by the application and the server when the connection is created.

There are several Cipher Wizards to help you choose a set that is suitable for your use.

**Most Compatible** Select the settings found to be most compatible with the most servers.

**US Ciphers Only** Select only the US 'strong' (128 bit or greater) ciphers.

**Export Ciphers Only** Select only the weak (56 bit or less) ciphers.

**Enable All** Select all ciphers and methods.

Finally, there are some general SSL settings.

**Use EGD** If selected, OpenSSL will be asked to use the entropy gathering daemon (EGD) for initializing the pseudo-random number generator.

**Use entropy file** If selected, OpenSSL will be asked to use the given file as entropy for initializing the pseudo-random number generator.

**Warn on entering SSL mode** If selected, you will be notified when entering an SSL enabled site.

**Warn on leaving SSL mode** If selected, you will be notified when leaving an SSL based site.

**Warn on sending unencrypted data** If selected, you will be notified before sending unencrypted data via a web browser.

## 1.4 The OpenSSL Tab

Here you can test if your OpenSSL libraries have been detected correctly by KDE, with the Test button.

If the test is unsuccessful, you can specify a path to the libraries in the field labelled Path to OpenSSL Shared Libraries.

## 1.5 The Your Certificates Tab

The list shows which certificates of yours KDE knows about. You can easily manage them from here.

## 1.6 The Authentication Tab

Not yet documented

## 1.7 The Peer SSL Certificates Tab

The list box shows which site and personal certificates KDE knows about. You can easily manage them from here.