

CISX MDMS Technical Specifications

Revised: 7th September 2011

Table Of Contents

1 INTRODUCTION.....	3
1.1 INTENDED AUDIENCE.....	3
1.2 ABBREVIATIONS.....	3
2 OVERVIEW.....	3
3 SYSTEM REQUIREMENTS.....	3
3.1 OPERATING SYSTEM REQUIREMENTS.....	3
3.2 HARDWARE REQUIREMENTS.....	3
3.2.1 CPU.....	3
3.2.2 RAM.....	3
3.2.3 Disk Space.....	3
3.2.4 Display.....	4
3.3 NETWORK REQUIREMENTS.....	4
4 TECHNICAL SPECIFICATIONS.....	4
4.1 PROGRAMME DEVELOPMENT LANGUAGE.....	4
4.2 COMMUNICATION.....	4
4.2.1 Host Name Resolution	4
4.2.2 Connections.....	5
4.2.2.1 Permanent Connection.....	5
4.2.2.1.1 Application Protocol.....	5
4.2.2.1.2 SSL Protocol Overview.....	5
4.2.2.2 Temporary Connections.....	6
4.2.3 Proxy Servers.....	6
4.3 LOCAL FILE CREATION.....	7
4.4 REGISTRY ENTRIES.....	7
4.4.1 User configurable registry keys.....	7
4.5 PROGRAMME BUG REPORTING.....	9

1 Introduction

This document details the technical specifications of the Contributor Market Data Management Services software as provided by the Channel Islands Stock Exchange.

1.1 Intended Audience

The intended audience of this document are the information technology staff of Contributors, or their agents, that are responsible for installation of software for use by their internal staff.

1.2 Abbreviations

The following abbreviations are referred to throughout the document.

- CISX – Channel Islands Stock Exchange.
- MDMS – Market Data Management Services.
- SSL – Secure Sockets Layer.
- TLS – Transport Layer Security.
- RSA – Rivest, Shamir and Adleman. A public key algorithm for asymmetric encryption.
- RC4 – Rivest Cipher 4 (also known as ARC4 or ARCFOUR). A streaming symmetric encryption algorithm.
- SHA – Secure Hash Algorithm.
- OS – Operating System.
- DNS – Domain Name System.
- HTTP – Hypertext Transfer Protocol.
- HTML – Hypertext Markup Language.
- TCP/IP – Transmission Control Protocol / Internet Protocol.
- COM – Component Object Model.

2 Overview

The Contributor MDMS application is bespoke software created by the CISX, which allows Contributors to publish market data directly to the CISX systems.

3 System Requirements

3.1 Operating System Requirements

The software runs under the following Microsoft operating systems:

Windows 2000 (SP4)

Windows XP (SP1, SP2, SP3)

Windows 7

The software has been tested on Windows XP Professional (SP3) and
The software has been tested on Windows 7 Professional.

3.2 Hardware Requirements

3.2.1 CPU

IA-32 (Pentium Pro and above) or compatible, PIII or above recommended.

3.2.2 RAM

128MB + OS memory requirements, 256MB or above recommended.

3.2.3 Disk Space

114 MB free before installation.

3.2.4 Display

800x600x256 colours minimum, 1024x768x64k colours or above recommended.

3.3 Network Requirements

A connection to the Internet with a bandwidth of 64kb/s or better.

Access to the following host addresses:

www.cisx.com

marketdata.cisx.com

NOTES:

In demonstration mode please replace reference to host name *marketdata.cisx.com* with *develop.cisx.com* .

Ports and protocols used for communication are detailed in section 4.2 Communication.

4 Technical Specifications

4.1 Programme Development Language

The software was developed using Java SE 6.0 and compiled to binary executable image for Windows using Excelsior JET, which is a certified Java SE 6.0 implementation powered by ahead-of-time compilation technology. Visit <http://www.excelsior-usa.com/jet.html> for further details. This technology helps:

- Speed up Java applications without any source code changes or hardware upgrades.
- Protect Java code from decompilation without compromising its performance.
- Build compact and professional installers for Java applications without dependency on a Java Runtime Environment (JRE).

4.2 Communication

The software uses four forms of communication outside the realm of the user interface.

- Communication with the local machine for name services, used to establish host-name resolution.
- Communication with the CISX, a permanent connection for the purpose of receiving and sending market data information.
- Communication with the CISX for the reading of the CISX market news web-site cascading style sheet. This is achieved on a temporary connection basis and is not critical to the operation of the software, should a connection of this type not be possible.
- Communication with the CISX for the reading a web-based Javascript HTML editor, found on the CISX web-site. This is only required when the IE Browser based HTML editor option is chosen from within the application. The default HTML editor does not have this requirement.

4.2.1 Host Name Resolution

The software uses naming services to establish the IP addresses for the following host names: *marketdata.cisx.com* and *www.cisx.com*.

Host name-to-IP address *resolution* is accomplished through the use of a combination of local machine configuration information and network naming services such as the DNS and Network Information Service (NIS). The particular naming services(s) being used is by default the local machine configured one.

Special note: host name resolution does not have to be available or configured on the local machine when a proxy server is used for establishing the permanent connection.

4.2.2 Connections

4.2.2.1 Permanent Connection

During the runtime of the application the software will attempt to establish a permanent connection to the CISX.

By default the software will attempt to connect to host address *marketdata.cisx.com* on port 5432 using a proprietary application protocol layered on a TCP/IP stack.

4.2.2.1.1 Application Protocol

The application layer protocol is proprietary to PostgreSQL (see <http://www.postgresql.org> for further details). Essentially it is layered on top of a TCP/IP stack with SSL.

The following diagram shows the essential layers.

TCP/IP Protocol Stack With SSL

<i>TCP/IP Layer</i>	<i>Protocol</i>
Application Layer	PostgreSQL proprietary protocol (http://www.postgresql.org)
Secure Sockets Layer	SSL
Transport Layer	TCP
Internet Layer	IP

4.2.2.1.2 SSL Protocol Overview

SSL is the most widely used protocol for implementing cryptography on the Internet. SSL uses a combination of cryptographic processes to provide secure communication over a network. This section lists the cryptographic processes that the software uses.

The SSL version used by the software is version 3.0. SSL is defined in [1] *The SSL Protocol version 3.0 Internet Draft*.

The key exchange protocol uses RSA at 768 bits (the number of bits is set by the CISX server and can be increased at any time). RSA is defined in [2] *RSA*.

Authentication of the public key received is achieved by checking the signature of the certificate containing the public key.

A certificate is a general term for a signed document containing a name and public key information. Such a certificate can take many forms but the CISX signing is based on the X.509 certificate format. X.509 is defined in [3] *X.509 Certificates*.

Only public key certificates signed by the certificate authority (CA) used to sign the CISX server certificates is accepted. (The public key of the CA used to sign CISX server certificates is embedded in the software for this purpose).

This technique ensures that the software will only connect to an authentic CISX server as frauds attempting to spoof a CISX server would also have to know the private key of the CA certificate, which is not public information and highly improbable to reproduce.

The cipher encryption protocol uses RC4 at 128 bits. RC4 is defined in [4] *RC4*.

The hash message authentication code (HMAC) protocol uses SHA1 (160-bit digest). SHA1 is defined in [5] *Secure Hash Algorithm 1*.

The implementation of all security algorithms are provided by Sun Microsystems in the Java Secure Socket Extension (JSSE) (refer to [6] *JSSE*).

Notes:

In software versions 4.0.3 and earlier, key exchange for the RC4 128 bit cipher key is performed only once during initial SSL handshake.

In all later versions of the software key exchange is performed periodically at 5 minutes intervals.

References:

[1] *The SSL Protocol version 3.0 Internet Draft:*

<http://wp.netscape.com/eng/ssl3/ssl-toc.html>

[2] *RSA:*

<http://www.ietf.org/rfc/rfc2313.txt> which is superseded by

<http://www.ietf.org/rfc/rfc2437.txt>

[3] *X.509 Certificates:*

<http://www.ietf.org/rfc/rfc2459.txt>

[4] *RC4:*

<http://www.mozilla.org/projects/security/pki/nss/draft-kaukonen-cipher-arcfour-03.txt>

[5] *Secure Hash Algorithm 1:*

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>

[6] *JSSE:*

<http://java.sun.com/j2se/1.5.0/docs/guide/security/jsse/JSSERefGuide.html>

4.2.2.2 Temporary Connections

When the user is creating, amending, editing or approving market news, via the integrated HTML editor for market news, a temporary connection is made for reading the cascading style sheet file: <http://www.cisx.com/cisxnews.css>.

The temporary connection is made over port 80, using the HTTP protocol to host address www.cisx.com.

If this file cannot be obtained through a connection, default style sheet values are used. In this case the resulting HTML news displayed in the editor may look less like what it should look like when displayed on the CISX web-site.

When the user is creating, amending, editing or approving market news, via the IE Browser based HTML editor for market news, a temporary connection is made for reading the web-page and related content (Javascript) into the IE Browser (embedded into the application via COM automation).

Web page: <http://www.cisx.com/mdmseditor/editor.php>.

The temporary connection is made over port 80 using the HTTP protocol to host address www.cisx.com.

If this web-page cannot be loaded through a connection, creating, amending, editing or approving market news will not be possible. One can always revert to the default integrated HTML editor.

4.2.3 Proxy Servers

The software can be configured to connect indirectly to the CISX via proxy servers.

The software's default setting is not to use a proxy server, but should one be required the software can communicate via SOCKS or HTTPS proxy server protocols.

For a SOCKS server, only SOCKS version 4 or 5 are supported and it has to allow for unauthenticated connections.

When specifying an HTTPS proxy server the port for making a permanent connection to the CISX will automatically be set to 443.

Should authentication be required, the only type of authentication supported for this type of connection is BASIC.

Not all HTTPS proxy servers will allow tunnelling to *marketdata.cisx.com* on port 443 using SSL. The reason for this is due to the proprietary protocol used. Before a SSL handshake can commence, 8 bytes of data must be sent to the CISX server, which must reply with a single byte response. Some "intelligent" proxy servers check for the SSL handshake and will deem these first bytes of data exchange as invalid.

4.3 Local File Creation

During runtime of the application the software may create the following files.

- `<%USERPROFILE%>\spellyxcustom.dict`
This is a permanent file and is created when the user adds custom words to the spell checker of the integrated HTML editor.
The HTML editor is activated when creating, amending, editing or approving market news.
- `<%TEMP%>\cisxapp\news_?.html`
This is a temporary file created when previewing market news. Its contents will be HTML text. Its life expectancy will be no longer than that of the running application. That is, if it still exists when the application is closing down, it will be deleted.
- `<%TEMP%>\cisxapp\news_?.pdf`
This is a temporary file created when previewing market news that has a PDF attachment. Its contents will be PDF data. Its life expectancy will be no longer than that of the running application. That is, if it still exists when the application is closing down, it will be deleted.

4.4 Registry Entries

During runtime of the application the software will read and write settings to the registry. There are two base registry keys that the application uses and they are:

`HKEY_CURRENT_USER\Software\JavaSoft\Prefs\applications\ /C/I/S/X\`
Data is written to this node during normal operation of the application.

`HKEY_LOCAL_MACHINE\Software\CISX\MDMS\Options`
Data is written to this node when a Windows Administrator chooses to lock the Network Settings data and optionally changes any locked network settings.

4.4.1 User configurable registry keys

All registry keys can be configured via the software. However should one choose to configure settings via group policies or the likes the following is a description of the values for setting network options.

Root key: `HKEY_LOCAL_MACHINE\Software\CISX\MDMS\Options`

Value Name: `dbport`

Type: `REG_SZ`

Values: `5432` or `443`

Notes: These are the ports that CISX server software listens for network connections on. The only acceptable values are `5432` or `443`, as these are the only ports that the CISX will accept connections on.

The default value when not specified is 5432.

Value Name: Locked

Type: REG_SZ

Values: true or false

Notes: When set to `true` ONLY a Windows Administrator can change network settings from within the application software and the network settings will be GLOBAL to all users that use the software.

When set to `false` these settings are not used for network connections. The settings that will be used are on a per-user profile base and are found under key:

HKEY_CURRENT_USER\Software\JavaSoft\Prefs\applications\C/I/S/X/options

When set to `false` any user of the software can change the network settings.

Value Name: proxy

Type: REG_SZ

Values: HTTPS, SOCKS or None

Notes: When set to `HTTPS` the application software will attempt to connect to the CISX via a secure tunnel through a proxy sever.

When set to `SOCKS` the application software will attempt to connect to the CISX via a Socks sever. If this option is set to either `HTTPS` or `SOCKS` then the `proxyHost` and `proxyPort` settings must also be set.

Value Name: proxyHost

Type: REG_SZ

Value:

Notes: This value is the address of the proxy server and must set when setting `proxy` is also set. The value can either be a canonical name such as `proxy.servers.net` or an IP address such as `192.168.1.1`.

Value Name: proxyPort

Type: REG_SZ

Value:

Notes: This value is the port to connect on when a connection via a proxy server is required and must set when setting `proxy` is also set.

The value must be a numerical number, for example 3222.

Value Name: proxyUser

Type: REG_SZ

Value:

Notes: This value is optional and is the "user name" used if BASIC authentication is required for connections via a proxy server.

Value Name: proxyPassword

Type: REG_SZ

Value:

Notes: This value is optional and is the "user password" used if BASIC authentication is required for connections via a proxy server.

The password must be stored using base64 encryption.

4.5 Programme Bug Reporting

The software utilises exception handling built into the Java language to capture unhandled exceptions.

Should an unhandled exception occur a bug report is generated, which will require user input to complete. On completion the report is sent to a CISX server (*marketdata.cisx.com*), using the same connection protocol as documented in section 4.2.2.1 Permanent Connection but, on a new temporary based connection for the sole purpose of sending the bug report.

The software captures all unhandled exceptions except "out of memory" exceptions.

Note that when an unhandled exception occurs, that relates to a connection type problem, it will not be possible to send a bug report.