

ML CLEARTM

Client Electronic Access & Reporting

User Guide for Trading Partners

Document Version 2.0

Table of Contents

1.	About CLEAR	4
2.	Getting Started	4
3.	Determine File Transfer Protocol	4
4.	Determine Data Exchange Method.....	5
5.	Generate Keys, Conduct Key Exchange.....	5
6.	Obtain User ID and Password.....	5
7.	Encrypt Data	5
7.1	Using Commercial Security Software.....	5
8.	CLEAR FTP Server Information.....	6
8.1	Servers	6
8.2	Directory Structure.....	7
9.	Sending & Receiving Data	7
9.1	General Procedure.....	7
9.2	Using your own software application or scripts.....	7
9.3	Using commercial FTP software	7
9.4	Using a command prompt.....	8
9.4.1	Initiate an FTP session	8
9.4.2	Sending	8
9.4.3	Receiving	8
9.5	Using a web browser.....	8
9.5.1	Sending	9
9.5.2	Receiving	9
9.7	Have CLEAR send data directly to your server or workstation.....	9
10.	Additional Information	10
10.1	Verification of Sent Files	10
10.2	Inbound Confirmation Process	10
10.2.1	Confirm.txt contents (tab-delimited)	10
10.2.2	Error.txt contents (tab-delimited).....	11
10.3	Your Responsibilities When Sending Files	11
10.4	File Naming & Time Stamping.....	12
10.5	Archives	12
11.	Technical Support.....	12
11.1	Download the GnuPG software	13
	Domestic (US) Users:	13
	International users:.....	13

11.2 Installation 13

11.3 Key Setup..... 13

 11.3.1 Keynames must be unique 16

11.4 Revocation Key..... 16

11.5 Export Key..... 17

11.6 Import Key..... 17

11.7 Sign the Merrill Lynch Key 17

11.8 Encrypting files for Merrill Lynch..... 18

 11.8.1 Using Options Files 18

11.9 Decrypting files from Merrill Lynch 19

11.10 Documentation..... 19

Contact Information

Email	+b2bsupportlevel2@exchange.ml.com
Internet Website	www.clear.ml.com
Phone Support	Domestic: 877-ML-CLEAR (877-652-5327) International: 212-647-3713

In connection with your use of the Merrill Lynch CLEAR **SM** service ("*ML Clear*"), you will need to download and/or utilize third party software (the "*Software*"). You agree that Merrill Lynch may, in its sole discretion and at any time, modify ML CLEAR, cease offering ML CLEAR or require the use of different software in connection with ML CLEAR. By obtaining/downloading the Software and using ML CLEAR you acknowledge and agree that: (a) MERRILL LYNCH DISCLAIMS ALL LIABILITY WITH RESPECT TO THE SOFTWARE AND MAKES NO REPRESENTATIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, OF ANY KIND WHATSOEVER WITH RESPECT TO THE SOFTWARE; (b) the Software has been developed and is owned by a third party and is subject to such third party’s terms and conditions of use and you will be solely and exclusively responsible for any failure by you or any person or entity acting on your behalf to comply with those terms and conditions; (c) Merrill Lynch shall have no obligation or duty to inform you of any updates, patches, fixes or problems with or to the Software; (d) you are responsible for complying with all laws, rules and regulations regarding the download and use of the Software; (e) you are responsible for the hardware related to and the software on your computers, systems and networks ("*Your Systems*"); (f) you are responsible for ensuring that the Software does not conflict with, change any of the desired settings on or damage Your Systems; (g) you should obtain/download the Software in accordance with your internal guidelines and procedures for obtaining/downloading software, including, if required, involving a system administrator or IT service person with such download; and (h) you will indemnify and hold us harmless from any damages arising from your download and use of the Software. Other terms and conditions to your use of ML Clear are included in your service level agreement with Merrill Lynch.

About CLEAR

Merrill Lynch CLEAR ("CLient Electronic Access and Reporting") is a utility for secure file exchange between Merrill Lynch internal business units (Subscribers) and their external clients (Trading Partners).

CLEAR works over both Internet and private network connectivity. Contact us if you are interested in using connectivity other than the internet. The ML CLEAR FTP servers are accessible through all Internet Service Providers (ISP's).

1. Getting Started

The following items must be addressed by Trading Partners in order to set up data exchange with Merrill Lynch – connectivity, encryption and the data exchange method. Each of the items in the list below is explained in detail in the following sections of this document.

1. Determine your file transfer protocol.
2. Determine your data exchange method (your own custom software, FTP, browser, etc.).
3. Generate secure keys if not already done so.
4. Conduct a key exchange.
5. Obtain a User ID and password from the CLEAR support group.
6. When sending data to Merrill Lynch, encrypt the data with your key before sending. When receiving data from Merrill Lynch, decrypt the data with your key.
7. Conduct testing for both sending and receiving files.

See the following sections for details on each of these steps.

2. Determine File Transfer Protocol

ML CLEAR support various file transfer protocols

- FTP w/ PGP (Preferred Method) – We support Open PGP standards to secure data during the file transfer
- FTP over VPN, Extranet, or Private Line. (Additional Cost for network infrastructure)
- AS2
- SFTP (SSH) – Server Only – ML CLEAR can not push files using SFTP
- FTPS (SSL)
- HTTPS

3. Determine Data Exchange Method

Determine your desired method for sending and receiving data. Your choices include:

- Your own in-house software application or custom scripts
- Commercial FTP software (CuteFTP, WS-FTP, etc.)
- Manual process using the command line or a browser

4. Generate Keys, Conduct Key Exchange

You may use any software you like to generate a key pair. Please refer to that software's user manual for information on generating keys.

This user guide gives you information on generating keys using GnuPG. See Appendix A.

5. Obtain User ID and Password

Contact the CLEAR support group to obtain a user ID and password.

Password change management must be coordinated with the CLEAR team.

6. Encrypt Data

If you are preparing to send data to Merrill Lynch, the next step in the process is to encrypt your data.

6.1 Using Commercial Security Software

CLEAR is compatible with OpenPGP, which is the most widely used encryption standard in the world, and is defined by the OpenPGP Working Group on the Internet Engineering Task Force (IETF) standard RFC 2440. The OpenPGP standard was originally derived from PGP (Pretty Good Privacy), first created by Phil Zimmermann in 1991. For more information on OpenPGP, refer to www.openpgp.org. The following products use the OpenPGP standard and are compatible with CLEAR:

Security Software	Comments
GnuPG (Privacy Guard)	GnuPG is a free alternative to PGP. Because it does not use the patented IDEA algorithm, it can be used without any restrictions. GnuPG is an RFC2440 (OpenPGP) compliant application. For further information, refer to www.gnupg.org .

Network Associates PGP	Commercial security software by Network Associates Inc. All versions are supported but only v6.5.8 or earlier works with the CLEAR-IDS software. Although the Network Associates PGP is no longer sold or supported by Network Associates Inc., if you already own this product, it is compatible with CLEAR.
McAfee E-Business Server	Commercial version supported by McAfee. Previously known as PGP E-Business Server
McAfee E-Business Server Partner Edition	Commercial version supported by McAfee. Command line version for fully automating processes
PGP Corp	www.pgp.com

See Appendix A for information on using GnuPG.

7. CLEAR FTP Server Information

Merrill Lynch has two internet-accessible FTP servers. Both servers are available at all times. The same data is available on both servers. Each login ID has a unique home directory structure which is listed in section 8.2.

7.1 Servers

Merrill Lynch recommends only using DNS to connect to our FTP server. All servers resolve to two separate IP addresses. Please ensure you have connectivity to both.

FTP Server **ftp.clear.ml.com**

PA Data Center 209.65.19.98

NY South Data Center 199.43.34.51

SFTP/FTPS Server **ftps.b2b.ml.com**

PA Data Center 209.65.19.96

NY South Data Center 199.43.34.44

Secure website **<https://www.clearb2b.ml.com>**

7.2 Directory Structure

/outgoing	Files being sent from a Merrill Lynch business unit to a Trading Partner will be available for pickup from this directory.
/archives	If you wish to have files archived, this option can be made available to you. If you opt for archiving, files will be moved from the outgoing directory into the archive directory at pre-determined times of day. Once moved into the archive directory, files will remain there for seven days and will then be purged. If archiving is turned off, files will not be moved – they will remain in the outgoing directory, but will be purged after seven days.
/incoming/BU	If you are sending files to a Merrill Lynch business unit, you will need to place the files in this directory, where “BU” is the business unit name. Each business unit destination has its own directory named after that unique destination (e.g., “/incoming/BCC” is the directory for the Merrill Lynch business unit known as Broadcast). You will have a separate “incoming/BU” directory for each business unit you send files to.

8. Sending & Receiving Data

8.1 General Procedure

- Access the ML CLEAR FTP Server: You must access the ML CLEAR FTP server using the standard ports for FTP as defined by [InterNic](#). These ports are port 20 (data port) and port 21 (command port). No other ports are allowed access to this FTP server.
- Sending: Encrypt your file(s). Then copy the file(s) into the “/incoming/BU” directory, where “BU” represents the name of the Merrill Lynch business unit to which you are sending.
- Receiving (Pickup): Pick up files from the “/outgoing” directory. CLEAR will have placed files from the business unit in this directory.
- Receiving (Delivery): If you opted to have CLEAR deliver files to your server or workstation, there is no action required on your part.

8.2 Using your own software application or scripts

You may wish to use your own software application or custom scripts to send and receive files. Use the CLEAR FTP server information, as well as your CLEAR User ID and password in your code.

8.3 Using commercial FTP software

You may wish to use commercial FTP software (such as CuteFTP, WS_FTP, FileZilla and others) to send and receive files. Configure this software according to the manufacturers’ user guides.

8.4 Using a command prompt

8.4.1 Initiate an FTP session

- After establishing an Internet connection, go to a DOS prompt. Enter the following command:

```
ftp ftp.clear.ml.com
```

- Enter the User ID and password assigned to you.

Your connection to the FTP site will be established. Once you have accessed the FTP site, you will see an incoming, an outgoing and an archives directory. Underneath the “/incoming” directory, there will be subdirectories named after the business units with which you exchange data.

- If you are initiating this session to send files, type “**bin**” at the FTP prompt to set the FTP file transfer mode to binary . (If an ASCII transfer is made, PGP will not be able to decrypt the encrypted files.) This will return “**Type set to I**”.
- If you are initiating this session to receive files and you do not want to be prompted yes/no when downloading each file, enter “**ftp -I**”.

8.4.2 Sending

- Encrypt your file.
- Set the prompt to the “/incoming/BU” directory.
- Type “**put filename**” where “filename” is the name of the file you wish to send.
- When you are finished, enter the “**bye**” command to close the session.

8.4.3 Receiving

- Set the prompt to the “/outgoing” directory.
- To retrieve all data from the outgoing directory, use the “**mget ***” command.
- To retrieve one specific file from the outgoing directory, use the “**get filename**” command, where “filename” is the name of the file you wish to retrieve.
- When you are finished, enter the “**bye**” command to close the session.

8.5 Using a web browser

Enter the following command into your browser’s Address or Location field:

```
ftp://UserID:password@ftp.clear.ml.com
```

8.5.1 *Sending*

- Open the “incoming/BU” directory for the business unit to which you wish to send a file.
- Encrypt the file(s) you want to send.
- Place a copy of the encrypted file into the “incoming/BU” directory. (You can use the “drag and drop” method, if desired.)

8.5.2 *Receiving*

- Open the “/outgoing” directory. This directory holds files which are outgoing from the Merrill Lynch business unit to you.
- Right click on the filename.
- In Internet Explorer, click “**Copy to Folder**”. In Netscape Navigator, click “**Save Link As**”.
- Specify the location where you would like the file to be stored.

8.7 **Have CLEAR send data directly to your server or workstation**

CLEAR can send data directly to your server or client workstation. The chosen machine must have an FTP Server running. Contact the CLEAR support team to set up direct delivery. You will need to provide the following information:

- Hostname
- IP Address
- User ID and Password (or designate anonymous FTP)

The User ID assigned to access your destination must be allowed the following functionality:

- Directory Listing (ls)
- Rename
- Read
- Write
- Delete

9. Additional Information

9.1 Verification of Sent Files

After files have been successfully delivered to an ML CLEAR FTP server, they are moved to a staging area for processing. This staging area is not an area accessible to you. If you wish to run a process to check your files after they have been delivered to the ML CLEAR FTP server – but before CLEAR picks them up for processing – do the following:

- When sending the file, add a “temp” prefix before the filename. Name the file “temp.filename” (where “filename” is the name of your file). The ML CLEAR FTP servers do not move files named “temp.*” to the staging area.
- Run your process to check and verify that the file has been delivered.
- After running your verification process, rename the file by removing the “temp” prefix so that ML CLEAR can move it to the staging area and process it.

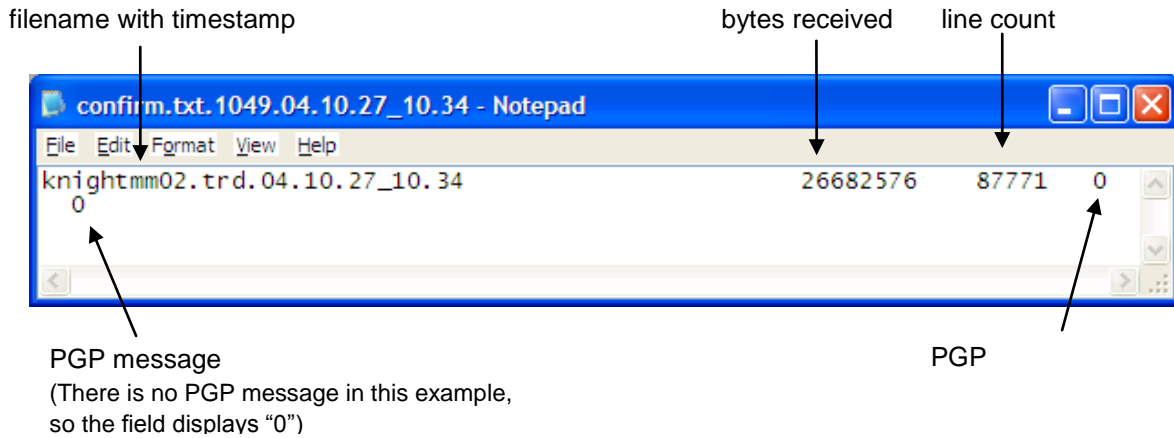
9.2 Inbound Confirmation Process

To confirm receipt of an inbound file (a file sent from you, inbound to Merrill Lynch), ML CLEAR sends a file to you called “confirm.txt”. If there was an error in the receipt, ML CLEAR will send a file to you titled “error.txt”. Check for this confirmation/error file to verify whether or not transmission to ML CLEAR was successful.

For MLX, the confirm and error files are pipe-delimited. For all other CLEAR implementations, the confirm and error files are tab-delimited and the layout is as follows:

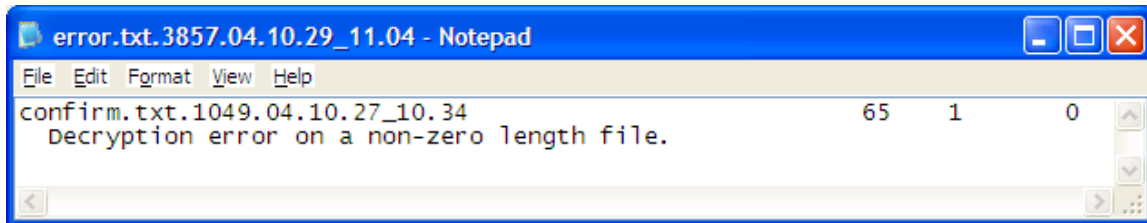
9.2.1 Confirm.txt contents (tab-delimited)

Line 1	Field 1	Decrypted filename with date/ time stamp (yy.mm.dd_hh.mm)
	Field 2	File size in bytes
	Field 3	line count
	Field 4	PGP Code
Line 2	Field 1	PGP message (if no message, then 0)



9.2.2 Error.txt contents (tab-delimited)

Line 1	Field 1	Original filename, no date/time stamp (yy.mm.dd_hh.mm)
	Field 2	File size in bytes
	Field 3	line count
	Field 4	PGP Code
Line 2	Field 1	PGP message (if no message, then 0)



9.3 Your Responsibilities When Sending Files

You are responsible for implementing a reliable FTP process. This process must include the following:

- Encrypting and signing files.
- Error checking of your FTP transmission process to insure successful FTP transmissions.
- You must check for the “confirm.txt” confirmation file. If this file is not received, a successful transmission to ML CLEAR was not made.
- When using the command line or your own software/scripts, use the “bye” command to properly close the FTP session.

9.4 File Naming & Time Stamping

All outbound filenames are created by the business unit sending the file. CLEAR adds two additional parameters to the filename.

.asc	This is the encryption extension added to all files. It cannot be shut off or changed. It is the same as .pgp
yy.mm.dd_hh.mm	(year.month.day_hour.minute) This is the timestamp that indicates when CLEAR has processed the file. This timestamp can be shut off but not rearranged.

9.5 Archives

Archiving is not automatic by default. If you wish to have your files archived, contact your ML CLEAR support team.

The archiving process can run once a day on the hour daily basis at pre-set times throughout the day. These times are as follows:

All files remain on the CLEAR FTP server for seven (7) days, whether or not you have selected the archiving option. The archiving option simply moves your files from the outgoing directory to the archive directory at one of the pre-set times dictated above. If you are receiving a large number of files each day, you may want to use the archiving option to cut down on the number of files displayed in your outgoing directory.

If you are using CLEAR-IDS, it is recommended that you leave the archiving option turned off. CLEAR-IDS does its own archiving.

10. Technical Support

All support is done based on the Merrill Lynch trouble ticket system (ITSM)

To open a ticket please call

Domestic US – 877-MLCEAR

International - 212-647-3713

Production support is provided 24 x 7 x 365.

For escalation of your ticket please contact

Phone 609-274-6261

Email +b2bsupportlevel2@exchange.ml.com

Appendix A: Encryption with GnuPG

This is information to assist you in using GnuPG without the CLEAR-IDS software. For instructions on using GnuPG with CLEAR-IDS, see the CLEAR-IDS User Guide.

10.1 Download the GnuPG software

Domestic (US) Users:

1. Go to <http://www.gnupg.org/>.
2. Click the Download link ([http://www.gnupg.org/\(en\)/download/index.html](http://www.gnupg.org/(en)/download/index.html)).
3. In the Binaries section, click on the “FTP” link next to the latest version of GnuPG compiled for Windows.
4. Save the zip file to your local disk.

International users:

1. Go to <http://www.pgpi.org/download/gnupg/>
2. Click on the latest version of GnuPG for Windows.
3. Pick the country you wish to download from.
4. Save zip file to local disk.

10.2 Installation

Extract contents of zip file into c:/gnupg (default).

If you do not use the default directory, you should enter a string with the directory into the Registry under the key:

```
\\HKEY_CURRENT_USER\Software\GNU\GnuPG\HomeDir
```

10.3 Key Setup

This step will create a key-pair and add it to your key-ring.

1. Open up command line and change directory to c:/gnupg.
2. Type: `gpg --gen-key`
3. Select Option **1** (DSA and ElGamal)
4. Enter key size **2048**
(You will be asked if you really want such a large key size. Answer **y**)
5. Select Never Expires (**0**)

6. Enter Key Name. The key name has three parts.

Real Name – Enter your company name

Email Address – Enter the email of the main contact person at your company

Comment – Can be something like “This is our GPG key”

7. Enter Passphrase: You will be asked for your passphrase every time you sign data to be encrypted for Merrill Lynch or decrypt data you receive from Merrill Lynch. Select a passphrase that you will be able to remember and others will not easily guess. Keep your passphrase in a secure place. If you lose your passphrase, there is no way to recover it.

A typical key-generation session (user responses in bold print) is displayed on the following page.

```
C:\GnuPG>gpg --gen-key
gpg (GnuPG) 1.0.6; Copyright (C) 2001 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
  (1) DSA and ElGamal (default)
  (2) DSA (sign only)
  (4) ElGamal (sign and encrypt)
Your selection? 1
DSA keypair will have 1024 bits.
About to generate a new ELG-E keypair.
           minimum keysize is 768 bits
           default keysize is 1024 bits
           highest suggested keysize is 2048 bits
What keysize do you want? (1024) 2048
Do you really need such a large keysize? y
Requested keysize is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct (y/n)? y

You need a User-ID to identify your key; the software
constructs the User ID from Real Name, Comment and Email
Address in this form:
  "Heinrich Heine (Der Dichter)
  <heinrichh@duesseldorf.de>"

Real name: Joe Client
Email address: jclient@somecompany.com
Comment: My GnuPg Key
You selected this USER-ID:
  "Joe Client (My GnuPg Key)
  <jclient@somecompany.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.
```

After creating the key, you can check that the key has been placed into your keyring by typing:

```
gpg --list-keys
```

10.3.1 Keynames must be unique

Note: A key is fully specified by its entire name, e.g.

```
"Joe Client (My GnuPg Key) jclient@somecompany.com"
```

When referring to a key in a gpg command, you do not have to specify the entire key name. You need only specify enough to uniquely identify the key.

For example, if you have two keys:

```
"Mary Jones (some comment) mjones@ace.net"
```

```
"Sam Talbot (another comment) stalbo@allied.org"
```

you can specify the keyname with just "Mary" or "Sam"

Example:

```
gpg --encrypt ..... --recipient Mary
```

If you add another key:

```
Mary Perkins (some comment) <mperkins@ibm.com>
```

then Mary is no longer unique. You would then have to specify enough of the key name to uniquely specify it, e.g.:

```
gpg --encrypt ..... --recipient "Mary Jones"
```

Important Note: If the string you use to specify the key has embedded spaces, then the string must be enclosed in quotes.

10.4 Revocation Key

You can create this key for future use. If you ever want to stop using your key you send this key which revokes your current key from my keyring.

Use the gpg --gen-revoke command.

To revoke a key named "mykey", type:

```
gpg --output revoke.asc --gen-revoke mykey
```

10.5 Export Key

In this step, you are sending your public key to Merrill Lynch. (Remember, you should never send your private key to anyone.)

To create an export file for the key “**mykey**”, type:

```
gpg --armor --output mykey.asc --export mykey
```

The export file created (in the example “mykey.asc”) should be sent to mlclrcintsspt@win.ml.com.

10.6 Import Key

In this step, you are importing Merrill Lynch's public key into your keyring. This will allow you to encrypt files for Merrill Lynch.

Put the “**ml_dh_key.asc**” file in **c:/gnupg**

Type:

```
gpg --import ml_dh_key.asc
```

Check that the Merrill key has been added to your keyring by typing:

```
gpg --list-keys
```

10.7 Sign the Merrill Lynch Key

In this step, you inform gpg that you are confident that the “Merrill Lynch” key in your keyring is genuine. If you do not do this, gpg will bother you each time you try to encrypt for Merrill Lynch's key.

Type:

```
gpg --sign-key Merrill
```

10.8 Encrypting files for Merrill Lynch

To encrypt a file to sent to Merrill Lynch, you must specify the following information on the command line:

<code>--armor</code>	This will cause gpg to create an "ASCII-armored text file" which is the format normally used by our system. This also allows a comment to be attached to the encrypted file, if desired
<code>--output MyData.asc</code>	The name of the encrypted file to be written
<code>--recipient Merrill</code>	This tells gpg to use the "Merrill Lynch" public key to encrypt the file (Note: as mentioned above, if you have another key in your keyring which begins with "Merrill", then you have to specify more of the key name)
<code>--local-user "Joe"</code>	This tells gpg to use the "Joe Client.." private key to sign the file
<code>--sign --encrypt</code>	This tells gpg that you want to both sign and to encrypt the file

The last entry on the command line should be the name of the file to encrypt.

Example (this should all be typed on one line):

```
gpg --armor --output MyData.asc --recipient Merrill
--local-user Joe --sign --encrypt MyData.txt
```

You will be asked for your passphrase for the signing key ("Joe" in the above example).

10.8.1 Using Options Files

Note: You can save some typing by using options files.

If you will be regularly encrypting for Merrill Lynch and signing with the "Joe Client" key, then you can create an options file for that purpose.

In this example, we will call the file you create "EncryptForMerril.opt".

Commands in a options file are the same as on the command line, without the "--"

The options file (EncryptForMerril.opt for our example) would look like this:

```
armor
recipient Merrill
local-user Joe
sign
```

The command line to perform the same encryption specified above would now be:

```
gpg --options EncryptForMerrill.opt -encrypt MyReports.txt
```

10.9 Decrypting files from Merrill Lynch

Decrypting files is much easier, because gpg knows which key was used to sign the file and for which public key it was encrypted. All you have to tell it is where to write the decrypted file.

In the following example, the encrypted file received from Merrill Lynch is called `DataFromMerrill.asc`

```
gpg --output DataFromMerril.txt --decrypt DataFromMerrill.asc
```

This will create a cleartext (decrypted) file called `DataFromMerrill.txt`

You will be asked for your passphrase.

10.10 Documentation

The information presented above is intended to help new users with the functionality of GnuPg necessary to transmit data to and to receive data from Merrill Lynch. A full discussion of the GnuPg software and public key cryptography is beyond the scope of this document.

For more information, please refer to the documentation on the GnuPg website:

<http://www.gnupg.org/docs.html>

Also note that there is some documentation provided in the zip file from Gnu.

Specifically, the following files may be of interest:

README

README.W32

gpg.man