This document defines the components of PGP and FTP for encryption, authentication and FTP password changes.

It covers the generation and distribution of PGP keys, FTP Server user name and password distribution, encryption of the data, and use of digital signing.

There are technical specifications for the use of PGP, FTP, and TELNET as well as a list of suggested software for the clients to use.

PUBLIC/PRIVATE Key Pair Generation

- A PUBLIC/PRIVATE key pair will be generated for **GHP** use through a function provided by the PGP software. The PUBLIC key will be distributed to those who will be transmitting data to GHP. The transmitter will encrypt the data using the GHP PUBLIC key. This allows only the holder of the matching PRIVATE key (in this case GHP) to decrypt the data. Methods for distribution and verification of the PUBLIC key as well as authentication are discussed later in this document.

- A PUBLIC/PRIVATE key pair will be generated by the **receiver** for the **receiver of data** through a function provided by the **receiver's** client PGP software. The PUBLIC key will be distributed to GHP while the receiver of the data will hold the PRIVATE key. GHP will encrypt the data using the receiver's PUBLIC key. This allows only the holder of the matching PRIVATE key (in this case the **receiver of the data**) to decrypt the data. Methods for distribution and verification of the PUBLIC key as well as authentication are discussed later in this document.

- Methods available to GHP for out of band PUBLIC key distribution and verification.

  - **Fingerprint** (Part of the PUBLIC/PRIVATE key pair) uses the unique biometric words generated during the PUBLIC/PRIVATE key pair creation process. Calling the owner of the PUBLIC key on the telephone and confirming the list of words contained in the PUBLIC key verify the PUBLIC key. Tools provided in the PGP software display this information. The key must be exported for distribution. This allows the PUBLIC key to be downloaded or emailed to the transmitter of the data. After importing the PUBLIC key the key will be verified and signed for use through PGP software functions.
  - **Physical Delivery** of the exported PUBLIC key to the transmitter of data. After importing the PUBLIC key the key will be verified and signed for use through PGP software functions.

- Distribution of the FTP user name and password to the client must be secured.
  - Options for delivery of the name and password to the client.
    - Physical delivery
    - Relay the information over telephone
    - Email the information in a PGP encrypted text file.
  - Clients will be required to change their password at first login attempt.
  - Client passwords will automatically expire after 180 days. The client must login to renew the password.
  - Minimum password length is set to eight characters.

- FTP client password changes must be processed by logging on to the FTP Server using TELNET/SSL or HTTPS using standard Internet browser with SSL support.

  - Requires Client to use one of the following methods to maintain password.
    - TELNET/SSL option
      - Requires a Client TELNET using SSL to login to Server
      - User password is changed through FTP Server menu selections.
    - HTTPS using standard Internet browser with SSL support.
      - Requires standard Internet browser with SSL support.
      - User password is changed through FTP Server menu selections.

Method of data encryption using PUBLIC/PRIVATE keys, and user authentication using FTP Server Security and digital signing. The following information is based on the assumption that the PUBLIC/PRIVATE keys have been created and distributed using the methods above.

- Data transmission between GHP and Client using data encryption and user authentication through the FTP Server login **and *digital signing***.

  - Data being sent from GHP to client.
    - Then the data is encrypted by GHP using the Client (receiver of data) PUBLIC key as well as digitally signed with the GHP PRIVATE key and sent to the clients outbox on the FTP Server.
    - The data is transmitted to a secure mailbox on the GHP FTP Server and is only accessible to the client by logging on using the FTP Server user name and password assigned to the client.
    - This is a FTPS (FTP + SSL) connection so the user name and password is encrypted at all times.
    - The client (receiver of data) is the only one able to decrypt the data because the client is the holder of the PRIVATE key. The digital signature of the sender is verified by the using the sender's PUBLIC key.
    - The client knows the data originated from GHP because the client is logging on to the GHP FTP Server to retrieve the data. Also because the data was digitally signed with the GHP PRIVATE key, the client can be sure the data came from GHP.

  - Data being sent to GHP from client.
    - The data is encrypted by the client (sender of the data) using the GHP (receiver of data) PUBLIC key and digitally signed using the sender's PRIVATE key and sent to the client's inbox on the FTP Server.
    - The data is available only to the client by accessing the FTP server and logging on using the FTP Server user name and password assigned to the client and internal GHP processes.
    - This is a FTPS (FTP + SSL) connection so the user name and password is encrypted at all times.
    - GHP (receiver of data) is the only one able to decrypt the data because GHP is the holder of the PRIVATE key.
    - GHP (receiver of data) decrypts the data using the GHP the PRIVATE key. The digital signature of the sender is verified by the using the sender's PUBLIC key.
    - GHP knows the data originated from the client because the client is authenticated using the GHP FTP Server. Also because the data was encrypted with the client PRIVATE key, the GHP can be sure the data came from the client.

- Technical specifications for PGP software.
    - PGP VERSION 8 OR COMPATIBLE
    - KEY PAIR TYPE Diffie/Hellman/DSS
    - KEY PAIR SIZE 4096 bits
    - KEY PAIR EXPIRATION Never (Key expiration/revocation will be controlled and audited by an administrative process)
    - PASSPHRASE More than 8 characters and numbers
    - SEND TO ROOT SERVER No
    - CIPHER CAST

- Suggested PGP client software in the process of testing.
    - PGP Desktop for GUI interface
    - PGP Personal for GUI interface
    - FileCrypt for batch script processing
    - NAI E-Business Server for batch script processing

- Technical specifications for TELNET/SSL software.
    - TELNET + SSL Capable
    - IMPLICIT Connection to Port 992

- Suggested TELNET/SSL client software in the process of testing.
    - **PUTTY – Freeware**
    - **Web Site** - http://www.chiark.greenend.org.uk/~sgtatham/putty/
        - No Cost

- Technical specifications for FTP software.
    - FTP + SSL Capable
    - IMPLICIT Connection to Port 990
    - PASSIVE Mode
    - Authorize Data Channel through PROT P Command after LOGIN

- Suggested FTPS client software in the process of testing.
    - **HTTPS using standard Internet browser with SSL support.**
    - **SmartFTP – Secure FTP GUI only Client from Smartftp.com Inc.**
        - **Web Site** - http:// http://www.smartftp.com/
        - Cost $30.00
        - Testing is complete and successful from the Internet using AOL access and internal.
        - Only GUI exists.
        - Configure FTP Site connection parameters
            - Select SSL Implicit mode by selecting address tab on tool bar and selecting SSL implicit mode
            - Set site name – wcp1.thehealthplan.com
            - Set username and password
            - Set passive mode
    - **MoveIT – Secure Command-Line FTP Client from Standard Networks**
        - **Web Site** - http://www.stdnet.com/
        - No cost for this product.
        - Testing is complete and successful from the Internet using AOL access and internal.
        - Batch mode command line interface. No GUI exists
        - Add GHS DNS Server to network configuration for Internet access.
        - Logon with following command
            - ftps -a -d -e:implicit wcp1.thehealthplan.com or through a script file.
              C:\temp\wildcat_maxim\movit_freely\movit_freely_sample.bat
        - After login Authorize Data Channel through PROT P Command
        - Sample scripts are movit_freely_sample.bat and movit_freely_sample.ftp

- **CuteFTP Pro Secure FTP GUI only Client from Globalscape.**

  - **Web Site** - http://www.globalscape.com/store/
  - Cost $105.00
  - Testing is complete and successful from the Internet using AOL access and internal.
  - Only GUI exists.
  - Logon with following command
    - For GUI "C:\Program Files\GlobalSCAPE\CuteFTP Pro\cftppro.exe"
  - Configure site through GUI Organize Sites Menu option
    - Set site name – wcp1.thehealthplan.com
    - Set username and password
    - Set passive mode
    - Set server type implicit/ssl connection
    - Set local folder

- **WS-FTP Pro – Secure FTP Client from Ipswitch Inc.**

  - **Web Site** - http:// http://www.ipswitch.com/
  - Cost $50.00
  - Testing is complete and successful from the Internet using AOL access and internal.
  - Both batch mode command line interface and GUI exists.
  - Add c:\program files\ws_ftp pro to system path
  - Logon with following command
    - For GUI C:\Program Files\WS_FTP Pro\wsftppro.exe or through a script file ftpscrpt -f c:\temp\wildcat_maxim\ws_ftp_pro\ws_ftp_sample.scp
  - After login Authorize Data Channel through PROT P Command
  - Sample scripts are ws_ftp_pro_sample.bat and ws_ftp_pro_sample.ftp
  - Configure site through GUI Organize Sites Menu option
    - Set site name – wcp1.thehealthplan.com
    - Set username and password
    - Set passive mode
    - Set server type implicit/ssl connection
    - Set local folder
    - Set command prot p

Along with FTPS (FTP w/ SSL) we have recently added SFTP (FTP w/ SSH) to our inbound server for file transfers. The SFTP server software uses port 22 for connections to us and we are using SSH public keys along with a password for authentication to the server. Below are some of the software that work with SFTP.

SFTP client software.

- **CuteFTP Pro Secure FTP GUI only Client from Globalscape.**
  - Web Site - http://www.globalscape.com/store/
  - Cost $105.00
  - Only GUI exists.
- **WS-FTP Pro – Secure FTP Client from Ipswitch Inc.**
  - Web Site - http://www.ipswitch.com/
  - Cost $50.00
  - Both batch mode command line interface and GUI exists.
- **WinSCP**
  - Web Site - http://winscp.sourceforge.net/eng/
  - No Cost for this Product
  - Both Command Line and GUI interface exists.