

# Encryption/Decryption & File Naming

## Middleware File Transport Services (External)

### Scope

This document illustrates the file transport services (FTS) and has been divided into individual sections that detail specific aspects of the services.

### Contents

Key Terms	2
File Transport Services External Processing Definitions	3
Process Parameters	3
Management of Inbound Files to CalPERS	3
Management of Outbound files from CalPERS	4
File Naming Convention	5
Examples of Proper File Naming	5
Related Resources	6
Revision History	6

## Key Terms

For the purposes of this document, the following terms and definitions apply.

Key Term	Definition
OpenPGP	Non-proprietary format for authenticating or encrypting data, using public key cryptography.
GnuPG	(GNU Privacy Guard) The free equivalent of OpenPGP. Based on the OpenPGP standard, encrypted GnuPG data can be decrypted by PGP and vice versa.
Public Key	A public key is the publicly disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

## File Transport Services External Processing Definitions

The business partner will be provided a secure login account to the CalPERS external SFTP server.

### Process Parameters

#### For Inbound Only

The external partner will be provided with one folder – PROD-IN. This folder will be used to retrieve files from CalPERS.

#### For Outbound Only

The external partner will be provided with one folder – PROD-OUT. This folder is used for sending files to CalPERS.

#### For Bidirectional (Inbound and Outbound)

The external partner will be provided with two folders – PROD-IN and PROD-OUT.

- The PROD-IN folder is used to retrieve files from CalPERS.
- The PROD-OUT folder is used for sending files to CalPERS.

### Management of Inbound Files to CalPERS

- Data files must be encrypted with the CalPERS public key using any OpenPGP standard compliant software.
- Encrypted data files must be uploaded to the PROD-OUT folder on CalPERS' external file transfer protocol (FTP) server using binary mode.
- Data file names must be all lowercase and must match the data [file naming convention](#) outlined in this document.
- Two files must be provided for each transaction, one data file and one semaphore file. Both files will have the same name, but with different file extensions.
  - Data files will have a .pgp file extension.
  - Semaphore files will have a .sem file extension.
    - The semaphore file is an empty file that indicates the data file is complete and ready for further processing.

Example: Pair of files sent for each transaction:  
*filename.pgp* and *filename.sem*
- The CalPERS file transport service will poll the PROD-OUT folder for files at a pre-determined interval. The .pgp file and the matching .sem file will be deleted when successfully processed. Erroneous files that do not match the naming requirements will not be processed.

## Management of Outbound files from CalPERS

- Data files will be encrypted with the partner's public key using GnuPG (GPG) based on the OpenPGP standard.
- Encrypted data files will be uploaded to the PROD-IN folder on CalPERS external FTP server using binary mode.
- Data file names will be all lowercase and will match the data [file naming convention](#) outlined in this document.
- Two files will be uploaded for each transaction, one data file and one semaphore file. Both files will have the same name, but with different file extensions.
  - Data files will have a .pgp file extension.
  - Semaphore files will have a .sem file extension.
    - The semaphore file is an empty file that indicates the data file is complete and ready for further processing.

Example: Pair of files sent for each transaction:  
*filename.pgp* and *filename.sem*
- The CalPERS file transport service will upload the encrypted data files to the FTP location at a pre-determined interval.
- The external partner will retrieve files from the FTP location at their own pre-determined interval.
- The external partner's application will look for a file name with a .sem file extension. This will indicate that a data file with the same name and a .pgp extension is available for processing. At this point, the partner's application can download the data file to the trading partner's system.
- After successfully downloading the data file, the trading partner's process will rename the data file from a .pgp extension to a .fin extension. This renaming process will indicate the files have been processed and can be deleted. The FTS cleanup service will delete the *filename.fin* and the *filename.sem* files.

## File Naming Convention

Both inbound and outbound files must adhere to the file naming convention described below and apply to both SFTP and file upload.

The standard format for file names is *yyyymmddhhmiss\_sss\_p(n).xxx*.

*yyyy* is the year

*mm* is the month

*dd* is the day

*hh* is the hours using a 24-hour clock

*mi* is the minutes

*ss* is the seconds

*sss* is the milliseconds (use 000 if milliseconds cannot be produced)

*p(n)* is the application specific area of the file name (project defined)

- Payroll Contribution files = 10006
- Retirement Enrollment files = 00007
- Health Enrollment files = 50031
- Deduction Register files = 20010
- Deduction Request files = 20016

*xxx* is the file extension

- .pgp = data encrypted FTP
- .sem = semaphore files

### Examples of Proper File Naming

Payroll - 20110321122800\_000\_10006.pgp

Retirement Enrollment - 20110321122800\_000\_00007.pgp

Health Enrollment - 20110321122800\_000\_50031.pgp

## Related Resources

For additional information, please refer to:

Resource	Relevance
<a href="#">myCalPERS Employer Technical Resources &amp; Toolkit Guide 2019 (PDF)</a>	Provides guidance on the technical resources available and more information about file submissions and transfers.

## Revision History

This document has been approved as follows:

Effective Date	Version	Approved by	Description of Changes
01/30/2009	0.1	Nate Eckler	Initial Draft
02/27/2009	1.0	Nate Eckler	Release V.1
03/24/2009	1.1	Nate Eckler	Not documented
06/02/2009	1.3	Shan Bains	Rewrite
01/06/2011	1.3.3	Shan Bains	Update cover page
04/12/2011	1.3.4	John Draper	Added example filenames on last page
02/07/2013	1.3.5	Amanda Poletti	General editing, no content change
01/22/2018	1.3.6	Rachael Lankford	Update formatting for accessibility mandate. No content changes.
11/20/2024	1.3.7	C. Powell	Updated template and format for accessibility compliance. Minor grammatical changes.