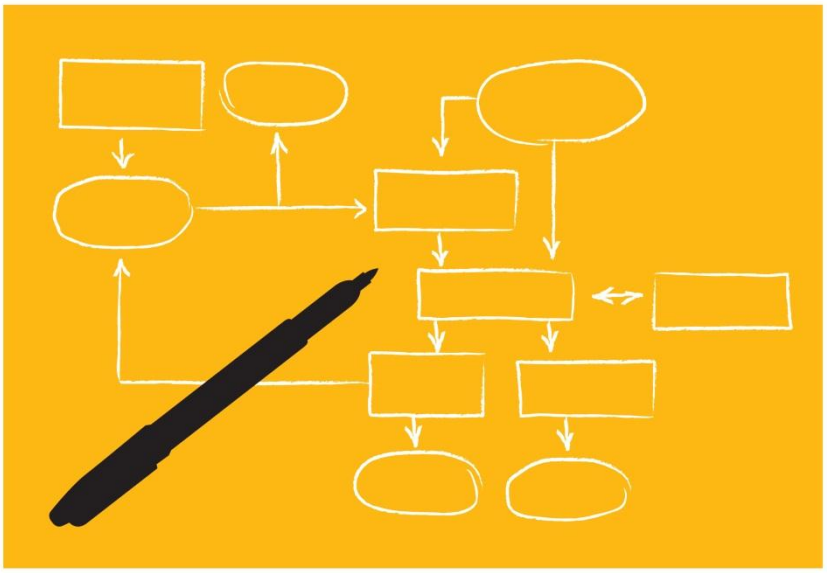

SAP NetWeaver 7.31

SAP NetWeaver Process Integration
Simple Use Cases for SFTP & PGP using Integration Flow Configuration

TABLE OF CONTENTS

1 PREFACE

1.1 Constraints

The texts, references, and graphics contained in this manual have been compiled with utmost care; nevertheless, it is impossible to guarantee that they are fully without error. SAP cannot assume any responsibility for the correctness or completeness of the following documentation; the user alone is responsible for verifying the information contained therein.
SAP will only assume liability for damage arising from the use of this documentation – irrespective of the pertinent legal basis – in the case of intentional or active negligence; under no other circumstances will a warranty be made.

1.2 Definition

This manual describes simple application cases of SFTP & PGP (B2B Adapter & Module) using Integration Flow configuration for process integration and all the configuration steps that are necessary to execute the application cases on the basis of SAP NetWeaver 7.31 SP04.

1.3 Intended Audience

This manual is intended to be used by both technology and application consultants.

1.4 Structure

The structure of this document follows the sequence of steps required to configure and run the use cases.

2 PREREQUISITES

2.1 General Prerequisites

To configure and execute the use cases, SAP NetWeaver with usage type Advanced Adapter Engine Extended must be correctly installed and configured. The following table lists the prerequisites and the relevant guides:

Step	Documentation
You have installed the Advanced Adapter Engine Extended.	• You can find the corresponding guides on SAP Service Marketplace in the Implementation Documentation Center for SAP NetWeaver 7.3 and SAP NetWeaver 7.3 including Enhancement Package 1
You have installed the SFTP & PGP Add-on.	• You can download the B2B add-on from the following location: http://service.sap.com/swdc -> Installation and Upgrades -> Browse our Download Catalog - > SAP NetWeaver and complementary products -> PI SFTP PGP ADDON. • Refer SAP NOTE: 1695521 for latest information on the download location of SFTP PGP Add-On. • For downloading latest Support package and patches, please refer to the following location. http://service.sap.com/swdc -> Support Packages and Patches -> Browse our Download Catalog -> SAP NetWeaver and complementary products -> PI SFTP PGP ADDON
You have imported the content for the Enterprise Services Repository corresponding to the latest support package/patch into the Advanced Adapter Engine Extended System.	• SAP Note 836200  The simple use cases are located in the Enterprise Services Repository in the software component *SAP BASIS,* software component version *SAP BASIS 7.31*, in the namespaces *http://sap.com/xi/XI/System/Patterns*.
You have configured the System Landscape Directory (SLD) for the Advanced Adapter Engine Extended System.	• Configuring, Working with and Administering System Landscape Directory

You have installed the NetWeaver Developer Studio.	• You can find the corresponding guides on SAP Service Marketplace at https://service.sap.com/installnw73 → Under Installation - Standalone Engines and Clients → Installation – Clients → Inst. and Update - SAP NetWeaver Developer Studio 7.3 EHP1 (SP04).

2.2 Providing the necessary User and Authorization

To log on to the PI 731 AEX system to configure the simple use cases, you have to create a user *XIDEMO* with the following roles:

- `SAP_XI_CONFIGURATOR_J2EE`
- `SAP_XI_MONITOR_J2EE`

To access (Read/Write) the file directories create the user XIDEMO on the system where the SFTP server is running.

2.3 Infrastructure

2.3.1 SFTP and PGP Certificates

This section describes how to create the SSH Certificates and the PGP Certificates:

➢ The following link describes

- How to create the SSH Certificates required to test the features of the SFTP Adapter
- Import the Private Key in the NWA key store
- Configure the Public Key in the SSH Server
- Verification of the Key pairs

http://wiki.sdn.sap.com/wiki/display/XI/Generating+SSH+Keys+for+SFTP+Adapters+-+Type+1

➢ The following link describes

- How to create the ASCII Armored PGP Certificates

http://wiki.sdn.sap.com/wiki/display/XI/Generating+ASCII+Armored+PGP+Key+Pairs

The ASCII armored PGP Certificates for the Sender and Receiver should be stored in a location in the PI host system.

Disclaimer: End User is free to use any other Third-party software.

2.3.2 Proxy Set-up

The execution of the variants `Variant03`, `Variant04` and `Variant05` require the HTTP and SOCKS proxy to be set-up and configured.

Also, create a user XIDEMO with access to the HTTP and SOCKS proxy.

2.3.3 Server Finger print

This section and the following link describes how to get the Server finger print for the SFTP server.
http://wiki.sdn.sap.com/wiki/display/XI/How+to+Determine+the+Public+Key+Finger+Print+of+a+SSH+Server

2.4 Setting up the File Directories in SFTP Server

The variants are based on the file directories accessible by in the system on which SFTP server is installed. When the use cases are executed, files are moved between file directories. Therefore, to be able to configure the use cases, the file directories must have been created and described in the SFTP server. Only then can you access the directories during configuration in the Integration Directory.

Perform the steps below to create the required directories on the system on which SFTP server is installed. Open the file directory.

1. Create a directory `SFTP&PGP` in which you can save files temporarily and create five sub directories `Variant01`, `Variant02`, `Variant03`, `Variant04`, `Variant05` in it.

.

A work directory already exists that can be used for this purpose and under which you can create the required directories.

2. Create one further sub directory `Input` in the sub directory `Variant01`.
3. Create two further sub directories `Input` and `Output` in `Variant02, Variant04,` and `Variant05`. And create three further sub directories `Input`, `Output1` and `Output2` in `Variant03`.
4. In the sub directory `Variant02` > `Input`, create one further sub directory `Delivery_Report`.
5. Futhermore, create a directory in the PI 731 Adavanced Adapter Engine Extended file share as `Archives` with two sub directories `Inbound_Message` and `Outbound_Message`.
6. Extract the following files to the the directory `SFTP&PGP`

- *ZXiPatternSenderFile1.xml*
- *ZXiiPatternSenderFile3.xml*
- *ZXiPatternSenderFile4.xml*
- XiPatternSenderFilesEOIO.zip (This file contains 1000 xml files for the EOIO scenario, they will be unpacked when executing the scenario.)

These files are provided by SAP in a ZIP file. The ZIP file for 7.31 containing also the EOIO test files is available in SAP Developer Network (SDN) and can be found using the direct link EHP 1 for SAP NetWeaver Process Integration 7.3 – Test Files for Simple Use Cases.

7. Copy the following files to the respective directories
    - *ZXiPatternSenderFile1.xml* and *ZXiPatternSenderFile3.xml* in `Variant03`
    - *ZXIPatternSenderFile4.xml* in `Variant02,Variant04` and `Variant05`.

2.5 Setting up the file directory in PI System to test the execution of OS Command in Variant01

To test the execution of the OS commands in PI System we need to have the .bat files configured to perform certain actions when triggered by the Sender and Receiver channels before and after the processing of the messages. The .bat files and output files that gets created from the execution of these .bat files needs to be placed in the file directory. Hence set up the file directory in the PI system by following the below steps.

1. Create a directory `OS-CMD` in which you can save files temporarily and place all the .bat files which contains the OS commands to be executed inside.

2. Extract the .bat files from the SFTP OS-CMD SU bat files.zip into the directory.

These files are provided by SAP in a ZIP file. The ZIP file for 7.31 containing also the EOIO test files is available in SAP Developer Network (SDN) and can be found using the direct link EHP 1 for SAP NetWeaver Process Integration 7.3 – Test Files for Simple Use Cases.

3. Open the .bat files in notepad and edit it by specifying the directory location which you have created to host the .bat files and the output files got by execution of these .bat files.

2.6 Creating the Technical and Business Systems in the System Landscape Directory of the PI System

Perform the following steps to create the required technical and business systems in the System Landscape Directory (SLD) for the PI 731 Adavanced Adapter Engine Extended System:

1. To call the System Landscape Directory for the System, open the Start Page using the URL: http://<Host>:<Port>/dir.
2. Start the SLD. To do so, on the start page, choose *System Landscape Directory*.
3. Log on using the *XIDEMO* user you created in 2.2.
4. On the initial screen of the SLD, choose *Technical Systems*.
5. Create a new technical system. To do so, choose *New Technical System.*
6. Select the type *Third Party* by choosing the appropriate radio button.
7. Choose *Next*.
8. On the *Technical System Wizard - System Details* screen, enter the following information about the technical system:
   - *Technical System Identification: Enter a name according to the following naming convention:* `<SID>_SFTP_PGP_TS`. In this case, `<SID>` is the **system ID of the PI System**.
   - *System Host Name*: Enter the **host name of the System**.
9. Choose Next.
10. To get the SAP delivered interfaces into the new business systems you need to add the SAP BASIS 7.31 component from product SAP EHP1 FOR SAP NETWEAVER 7.3 to the technical system.
11. Choose *Finish*. The System Details Section will open.
12. Now create the business systems. To do this, select the tab *Business Systems* in the System Details Section.
13. Choose *Add New Business System.*
14. The technical system should be preselected.
15. Choose *Next*.
16. Enter the name `<SID>_SFTP_PGP_BS1`. <SID> is the system ID of the Advanced Adapter Engine Extended System.
17. Choose *Next*.
18. The product SAP EHP1 FOR SAP NETWEAVER 7.3 should be already preselected.
19. Specify the System as Integration Server (field *Related Integration Server*).
20. Choose *Finish*.
21. Following the same procedure, create business systems with the following names:
    - `<SID>_SFTP_PGP_BS2`
    - `<SID>_SFTP_PGP_BS3`
    - `<SID>_SFTP_PGP_BS4`
    - `<SID>_SFTP_PGP_BS5`
    - `<SID>_SFTP_PGP_BS6`
    - `<SID>_SFTP_PGP_BS7`

2.7 Importing the Business Systems from SLD to the SAP Process Integration Designer

First, open the SAP NetWeaver Developer Studio
Set the connection data for accessing the Integration Directory under the menu *Process Integration* → *Change Preferences*. The connection details to the System have to be maintained using URL or Host and Port.

To call the SAP Process Integration Designer follow the menu path *Window → Open Perspective → Other → SAP Process Integration Designer*.
Logon to the system using the Menu *Process Integration → Connect* providing your user credentials
Perform the following steps to import the Business Systems:

1. In the menu select *Process Integration → Change Preferences*. The Preferences Window will appear.
2. Under *PI Tools configuration* select *Tool-Specific*.
3. Under *Update Local Cache Status* click the button *Update* to Refresh the SLD cache.
4. Click on *OK* button to close the window. On the Right bottom corner of NWDS the label “Updating cache” will appear & it will show the status progress. When the cache update has finished continue with the next steps.
5. On the Systems Entry in PI Explorer in the context menu select *Import Business System* to import the Business Systems into NWDS. A Window showing all available Business Systems in SLD will open.
6. Select the created Business Systems and click *Finish*.

3 VARIANT01: ONE SENDER & ONE RECEIVER– EXACTLY ONCE IN ORDER AND EXECUTION OF OS COMMANDS BEFORE AND AFTER THE MESSAGE PROCESSING BY SENDER & RECEIVER

This variant enables you to configure & execute a simple SFTP (Secure File Transfer Protocol) based message exchange with Quality of Service as- Exactly Once in Order.
For this a “Point-to-Point” -Integration Flow is configured with SFTP adapter on both sender & receiver channel sides.
Here the sender channel picks up a thousand xml files from an SFTP directory & sends it to the receiver channel which writes them to another SFTP directory. The messages are delivered in a particular order (here ascending by name).
The message is exchanged between sender and receiver adapter by using an Advanced Adapter Engine Extended. OS Commands configured are executed by the sender and receiver channels prior and post message processing.

3.1 Design Objects Used

The following describes all the design objects that describe the message exchange in this variant in turn. There are two possibilities to learn more about the design objects, the Enterprise Services Builder and the Enterprise Service Browser:

1. To call the Enterprise Service Browser in the SAP NetWeaver Developer Studio first set the connection data for accessing the Enterprise Services Builder under the menu *Window* > *Preferences*. Under *Web Services* > *Enterprise Services Browser* the connection details to the ESR System have to be maintained using ESR-Host and ESR-Port.

2. To call the Enterprise Services Browser follow the menu path *Window* > *Open Perspective* > *Other* > *Enterprise Services Repository.*

3. Use the Connect Button to connect to the Enterprise Services Builder.

4. In the navigation area, open the software component SAP BASIS, software component version SAP BASIS 7.31 and namespace-http://sap.com/xi/XI/System/Patterns.

5. Open the nodes Service Interfaces, Message Types and Operation Mappings to find the objects used in the scenarios.

All the design objects can also be checked directly in the Enterprise Services Builder. To call it call the Process Integration Tools Page http(s)://<AEX-Host>:<AEX-Port>/dir and from there open the Enterprise Services Builder.

3.1.1 Summary of Design Objects Used

The design objects used are summarized in the following table:

Object Type(Name)	Description
Service Interface (XiPatternInterface1O)	• Specifies the communication mode (asynchronous) and references the message type used.
Message type (XiPatternMessage1)	• Describes the message sent at runtime and references the data type used.
Data Type (XiPatternDataType1)	• Describes the data structure of the message.

3.2 Configuring the Process Integration Scenario

In configuration, you use the design objects for the actual system landscape. You have already described the system landscape in the SLD. The communication components you defined earlier enable you to address the involved business systems as senders/receivers of messages in the Integration Flow.
You perform the following configuration steps in the SAP Process Integration Designer for the Advanced Adapter Engine Extended.

3.2.1 Calling the Process integration Designer

First, open the SAP NetWeaver Developer Studio.

Set the connection data for accessing the Integration Directory under the menu *Process Integration* > *Change Preferences*. The connection details to the Advanced Adapter Engine Extended System have to be maintained using URL or AEX-Host and AEX-Port.

To call the SAP Process Integration Designer follow the menu path *Window* > *Open Perspective* > *Other* > *SAP Process Integration Designer*.

Logon to the AEX system using the menu path *Process Integration* > *Connect providing your user credentials.*

3.2.2 Creating the Integration Flow

Perform the following steps to create a new integration flow:

1. In the Process Integration Designer choose *New* > *Integration Flow (*  *)*.
2. In category Enterprise Integration Patterns select the Point-to-Point Channel Pattern and set the name or the Integration Flow as *XiPatternSFTPScenario_EOIO*.
3. Choose Next.
4. As Sender Business System select the Business System <SID>_SFTP_PGP_BS1 you imported from SLD using the Browse button.
5. As Interface select XiPatternInterface1O.
6. In Tab Receiver Systems as Receiver System select the Business System <SID>_ SFTP_PGP_BS2 using the input help for the Receiver Name.
7. As Receiver Interface select XiPatternInterface1_In.
8. Choose Finish.

9. The integration Flow will be displayed in a graphical overview.

3.2.3 Creating Channels

You perform the following steps to configure the connection of the process integration scenario. You activate the relevant sender-receiver relation (between the sender and receiver component) and assign both the sender and receiver a (sender or receiver) communication channel.

1. In the graphical editor, double click on channel for the sender component. The Details tab for the channel will open.

2. As Channel Name set *Sender*.

In the application *NWA > Communication Channel Monitoring* the channels can be filtered based on the value of the field *Channel ID.* (This is generated by appending the "Integration Flow name" + "_" + "the Channel Name"). In the above case it will be - *XiPatternSFTPScenario_EOIO_Sender*.

3. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

4. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > SFTP Server	• Server	• The Host Name/ IP Address on which SFTP server is running.
	• Port	• The SFTP server Port number. • By default **22** is set**. (It's the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific > Source > Proxy	• Proxy	• No Proxy
Adapter Specific > Source > Authentication	• Authentication Method	• Password
	• Username	• XIDEMO
	• Password	• Password for XIDEMO
Adapter Specific > Source > File	• File Name	• Wild card all. Set the value as **.* [a dot followed by a star]**
	• Directory	• Enter the path in the SFTP server's file directory that you defined previously (refer sec 2.4). • In this case of the sender communication channel, enter the whole path for the file directory *Variant01/Input*. Example: *~/<selected path>/SFTP&PGP /Variant01/Input*
Adapter Specific > Source > Period	• Poll Interval (min)	• 1

Adapter Specific > Processing > Processing Parameters	• Delete File	• Yes
	• Process Empty File	• Default
	• Process Sequence	• Ascending by name
Adapter Specific > Processing > Quality of Service	• Quality of Service	• Exactly once in order (asynchronous)
	• Queue Name	• QUEUE_SFTP
Adapter Specific > Processing > Run Operating System Command Before Message Processing	• Command Line	• cmd.exe /C <Path of the file directory which you have created in the section 2.5 to host Pre_Sender.bat file. • Example: cmd.exe /C "D:\usr\sap\PJ8\SYS\global\Connectivity_Test\B2B\SMR\SFTP\Pre_Sender.bat"
	• Timeout (secs)	• 10
Adapter Specific > Processing > Run Operating System Command After Message Processing	• Command Line	• cmd.exe /C <Path of the file directory which you have created in the section 2.5 to host Post_Sender.bat file.> • Example: cmd.exe /C "D:\usr\sap\PJ8\SYS\global\Connectivity_Test\B2B\SMR\SFTP\Post_Sender.bat"
	• Timeout (secs)	• 10

5. Now go back to the Graphical editor by clicking on the button ( ).

6. In the graphical editor, now double click on channel for the receiver component. The Details tab for the channel will open.

7. As Channel Name set *Receiver*.

8. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

9. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > SFTP Server	• Server	• The Host Name/ IP Address on which SFTP server is running.
	• Port	• The SFTP server Port number. • By default **22** is set**. (It 's the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific >	• Proxy	• No Proxy

Source > Proxy		
Adapter Specific > Source > Authentication	• Authentication Method	• Private Key
	• Username	• XIDEMO
	• Private key View	• SFTP_TEST (refer sec 2.3.1)
	• Private key Entry	• sftp_keystore (refer sec 2.3.1)
Adapter Specific > Source > File	• File Name	• XiPatternReceiverFile.txt
	• File Path	• Enter the path in the SFTP server's file directory that you defined previously (see 2.4). • In this case of the receiver communication channel, enter the whole path for the file directory *Variant01/Output*. Example: *~/<selected path>/SFTP&PGP /Variant01/Output*
	• Create Directory	• Yes
Adapter Specific > Processing > Processing Parameters	• Add Timestamp to filename	• No
	• Write Mode	• Append
Adapter Specific > Processing > Run Operating System Command Before Message Processing	• Command Line	• cmd.exe /C <Path of the file directory which you have created in the section 2.5 to host Pre_Receiver.bat file. • Example: cmd.exe /C "D:\usr\sap\PJ8\SYS\global\Connectivity_Test\B2B\SMR\SFTP\Pre_Receiver.bat"
	• Timeout (secs)	• 10
Adapter Specific > Processing > Run Operating System Command After Message Processing	• Command Line	• cmd.exe /C <Path of the file directory which you have created in the section 2.5 to host Post_Sender.bat file.> • Example: cmd.exe /C "D:\usr\sap\PJ8\SYS\global\Connectivity_Test\B2B\SMR\SFTP\Post_Receiver.bat"
	• Timeout (secs)	• 10

10. Now go back to the Graphical editor by clicking on the button ().

3.2.4 Saving, Activating & Deploying the Integration Flow

In the following steps, you save the integration flow with all its objects and activate it for the runtime.

1. Save the Integration Flow by pressing the save button ().

2. Use the Activate entry in the context menu of the integration flow *XiPatternSFTPScenario_EOIO* to activate the configuration.

3. Use the Deploy entry in the context menu of the integration flow *XiPatternSFTPScenario_EOIO* to deploy it in the runtime.

3.3 Executing the Use Case

You perform the following steps to check that the use case is executed without errors.

1. Stop the sender channel *XiPatternSFTPScenario_EOIO_Sender* in the *Configuration and Monitoring Home* > *Adapter Engine* > *Communication Channel Monitor* to make sure no processing runs during the time the files are placed into the source folder.

2. Open the configured directory *SFTP&PGP* on the SFTP server. (Refer section 2.4).

3. Unpack file XiPatternSenderFilesEOIO.zip in the subdirectory Variant01/Input. This will place a series of input files XiPatternSenderFile00001.xml, …, XiPatternSenderFile01000.xml.

4. The SFTP adapter is configured so that the files are picked in the order sorted by “ascending file names” and moved from the source directory *~/Variant01/Input* to the target directory *~/Variant01/Output* and the files are concatenated into a single file XiPatternReceiverFile.txt.

   

   On the SFTP server, open the file directory *~/Variant01*. If a folder- *Output* is already present, delete it. The execution of this test will create this folder.

5. Start the channel *XiPatternSFTPScenario_EOIO_Sender* in the *Configuration and Monitoring Home* > *Adapter Engine* > *Communication Channel Monitor* to start processing the files.

   

   Under the table “Processing Details” there will be a message- “Channel *** with id *** started at ***, next Execution scheduled at -***”.
   The sender channel will wait till the time for Next Schedule is reached. Then it starts processing.

6. Once the sender channel finishes processing open the directory ~/Variant01/Input and check that the all the input files should be deleted. As in the sender channel configuration we selected the “*Delete File*” checkbox.

7. Check that a Folder – *Output* is created under the folder *Variant01. Open it* and check that the files have been transferred.

8. Open the file XiPatternReceiverFile.txt and check whether the content is in the correct order.

9. The content must be in the correct order with the incremental ID value and the entire content must be present.

Furthermore, you can check the processing of the message in monitoring. To do this, proceed as follows:

1. Start the Monitoring by choosing Configuration and Monitoring Home on the Advanced Adapter Engine Extended start page.

2. Choose Message Overview.

3. Select Database.

4. Use appropriate filter criteria to restrict the number of XML messages displayed (for example, the processing period). On the very right hand side select Advanced to get all possible filter criteria

displayed. To select using your *Integration Flow* name use the input help for Integration Scenario under the section *Message Header Data*, put in the Integration Flow name *XiPatternSFTPScenario_EOIO* into the value field, press enter and select your Integration Flow.

5. Choose Go.

6. The system displays the filtered messages in a table.

7. Select any one message then click on *Open Message* Button. The tab *Payloads* displays the message content.

3.3.1 Verification of execution of Configured OS commands.

1. Go to the file directory which you setup under the section 2.5 on the PI Server.

2. Check whether four text files are created in the directory with the names Pre_Sender.txt, Post_Sender.txt, Pre_Receiver.txt and Post_Receiver.txt respectively.

3. These files are created before and after the processing of messages from sender and receiver communication channels.

4. Each text file should contain the Day, date and timestamp of the execution got by execution of the OS command.

5. This verifies the execution of OS commands successfully before and after the processing of messages from sender and receiver communication channels.

4 VARIANT02: ONE SENDER & ONE RECEIVER – SYNCHRONOUS COMMUNICATION

This variant enables you to configure & execute a simple SFTP (Secure File Transfer Protocol) based message exchange with Quality of Service as- Best Effort (synchronous communication).
For this a “Point-to-Point” -Integration Flow is configured with SFTP adapter on both sender & receiver channel sides.
Here the sender channel picks up an xml file from an SFTP directory & sends it to the receiver channel which writes it to another SFTP directory. In response the receiver channel sends a *Delivery Report.*
The message is exchanged between sender and receiver adapter by using an Advanced Adapter Engine Extended.

4.1 Summary of Design Objects Used

The design objects used are summarized in the following table:

Object Type(Name)	Description
Service Interface (XiPatternInterface2_Out_sync & XiPatternInterface2_In_sync)	• Specifies the communication mode (synchronous) and references the message type used.
Message type (XiPatternMessage2 & XiPatternMessage2Response)	• Describes the message sent at runtime and references the data type used.
Data Type (XiPatternDataType2 & XiPatternDataType2Response)	• Describes the data structure of the message.

4.2 Configuring the Process Integration Scenario

To configure this Variant a new Integration Flow is created.

4.2.1 Creating the Integration Flow

Perform the following steps to create a new integration flow:

1. In the Process Integration Designer choose *New > Integration Flow (*  *)*.

2. In category Enterprise Integration Patterns select the Point-to-Point Channel Pattern and set the name or the Integration Flow as *XiPatternSFTPScenario_SYNC.*

3. Choose Next.

4. As Sender Business System select the Business System <SID>_SFTP_PGP_BS1 you imported from SLD using the Browse button.

5. As Interface select XiPatternInterface2_Out_sync.

6. In Tab Receiver Systems as Receiver System select the Business System <SID>_ SFTP_PGP_BS2 using the input help for the Receiver Name.

7. As Receiver Interface select XiPatternInterface2_In_sync.

8. Choose Finish.

9. The integration Flow will be displayed in a graphical overview.

4.2.2 Creating Channels

You perform the following steps to configure the connection of the process integration scenario. You activate the relevant sender-receiver relation (between the sender and receiver component) and assign both the sender and receiver a (sender or receiver) communication channel.

1. In the graphical editor, double click on channel for the sender component. The Details tab for the channel will open.

2. As Channel Name set *Sender*.

   

   In the application *NWA > Communication Channel Monitoring* the channels can be filtered based on the value of the field *Channel ID.* (This is generated by appending the “Integration Flow name” + “_” + “the Channel Name”). In the above case it will be - *XiPatternSFTPScenario_SYNC_Sender*.

3. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

4. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > SFTP Server	• Server	• The Host Name/ IP Address on which SFTP server is running
	• Port	• The SFTP server Port number. • By default **22** is set**. (It ’s the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific > Source > Proxy	• Proxy	• No Proxy
Adapter Specific >	• Authentication Method	• Private Key

Source > Authentication	• Username	• XIDEMO
	• Private key View	• SFTP_TEST (refer sec 2.3.1)
	• Private key Entry	• sftp_keystore (refer sec 2.3.1)
Adapter Specific > Source > File	• File Name	• XiPatternSenderFile4.xml
	• Directory	• In this case of the sender communication channel, enter the whole path for the file directory *Variant02/Input*. (Refer section 2.4) Example: *~/<selected path>/SFTP&PGP /Variant02/Input*
Adapter Specific > Source > Period	• Poll Interval (min)	• 1
Adapter Specific > Processing > Processing Parameters	• Delete File	• No
	• Process Empty File	• Skip empty files
	• Process Sequence	• Default
Adapter Specific > Processing > Quality of Service	• Quality of Service	• Best effort (synchronous)
	• Response Directory	• Give the complete path for the folder -Delivery_Report. (Refer section 2.4) • Example: *~/<selected path>/SFTP&PGP /Variant02/Input/Delivery_Report*
	• Response Extension	• Response
Adapter Specific > Advanced > Archiving on SFTP Server	• Archive files on SFTP Server	• Yes
	• Archive name	• Archive
Adapter Specific > Advanced > Archiving on PI Server	• Archive files on PI Server	• Yes
	• Archive name	• Give the complete path for the folder - Outbound_Message. See section 2.4. Then append /%TIME_%SEQNUM at the end. • Example: ~/<selected path>/Archives/Outbound_Message/ %TIME_%SEQNUM

5. Now go back to the Graphical editor by clicking on the button ( ).

6. In the graphical editor, now double click on channel for the receiver component. The Details tab for the channel will open.

7. As Channel Name set *Receiver*.

8. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

9. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific >	• Server	• The Host Name/ IP Address on which SFTP server is running.

Source > SFTP Server	• Port	• The SFTP server Port number. • By default **22** is set**. (It 's the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific > Source > Proxy	• Proxy	• No Proxy
Adapter Specific > Source > Authentication	• Authentication Method	• Password
	• Username	• XIDEMO
	• Password	• Password for XIDEMO
Adapter Specific > Source > File	• File Name	• XiPatternReceiverFile.txt
	• File Path	• In this case of the receiver communication channel, enter the whole path for the file directory *Variant02/Output*. Example: *~/<selected path>/SFTP&PGP /Variant02/Output*
	• Create Directory	• No
	• Overwrite	• No
Adapter Specific > Processing > Processing Parameters	• Add Timestamp to filename	• No
	• Add Message-ID to filename	• Yes
	• Write Mode	• Direct
	• Set Permissions	• Yes
	• Permissions	• 600
Adapter Specific > Advanced > Archiving	• Archive files on PI Server	• Yes
	• Archive name	• Give the complete path for the folder - Inbound_Message. See section 2.4. Then append /%TIME_%SEQNUM at the end. • Example: ~/<selected path>/Archives/Inbound_Message/ %TIME_%SEQNUM

10. Now go back to the Graphical editor by clicking on the button ( ).

4.2.3 Saving, Activating & Deploying the Integration Flow

In the following steps, you save the integration flow with all its objects and activate it for the runtime.

1. Save the Integration Flow by pressing the save button ( ).

2. Use the Activate entry in the context menu of the integration flow *XiPatternSFTPScenario_SYNC* to activate the configuration.

3. Use the Deploy entry in the context menu of the integration flow *XiPatternSFTPScenario_SYNC* to deploy it in the runtime.

4.3 Executing the Use Case

You perform the following steps to check that the use case is executed without errors.

1. Open the configured directory *Input* under *~/SFTP&PGP/Variant02* on the SFTP server. (Refer section 2.4).

2. Rename the xml file to XiPatternSenderFile4.xml.

3. Once the sender channel finishes processing, check the *Input* folder, it should have a file *Archive-XiPatternSenderFile4.xml*. As in the sender channel we checked the option for Archiving on SFTP server.

4. Stop the sender channel *XiPatternSFTPScenario_SYNC_Sender* in the *Configuration and Monitoring Home > Adapter Engine > Communication Channel Monitor* to make sure no further processing.

5. Open the directory ~/Variant02/Output and check that the file is present & has the *Message ID* appended to its name.

6. Check the permission for the file. It should be as set in the Receiver Channel (600 – Read & Write for the Owner & No permissions for Group & Public).

7. As a response a Delivery report will be sent by the Receiver channel. Open the directory *Delivery_Report* under ~/Variant02/Input. A file XiPatternSenderFile4Response.xml should be present. Open the file it contains the details –Received File Name/Time/Date/Size/Destination.

8. Now check the “Archiving on PI server” feature. For this open the configured directory *Archives* on the host of the Advanced Adapter Engine Extended (refer prerequisites). The folder Outbound_Message & Inbound_Message should have the archived files.

Furthermore, you can check the processing of the message in monitoring as done in Variant01 above.

9. Now delete the content of the input xml file-XiPatternSenderFile4.xml (i.e. make it an empty file). Now start the sender channel. The file should not be picked & the message –“*File XiPatternSenderFile4.xml is empty.* It will be skipped.” will appear in the channel monitor for the sender channel. (As configured in the sender channel)

   

   Similarly in the Sender Channel editor you can set the value for *Empty file handling* under Adapter Specific > Processing > Processing Parameters as “Create no message” –In this case also – the file won’t be picked but no message will be generated.

5 VARIANT03: ONE SENDER & TWO RECEIVERS – WITH MAPPING

This variant enables you to configure & execute a simple SFTP (Secure File Transfer Protocol) based message exchange with Quality of Service as- Exactly Once (asynchronous communication).
For this an Integration Flow with “Recipient List” pattern is configured and has SFTP adapter on sender & both the receiver channel sides.
Here the sender channel picks up two xml files from an SFTP directory & based on the content sends it to the respective receiver channel which in turn writes it to another SFTP directory. A mapping is executed when the message is forwarded to one of the receivers.
The message is exchanged between sender and receiver adapter by using an Advanced Adapter Engine Extended.

5.1 Summary of Design Objects Used

The design objects used are summarized in the following table:

Object Type(Name)	Description
Service Interface (XiPatternInterface1 & XiPatternInterface2)	• Specifies the communication mode (synchronous) and references the message type used.
Message type (XiPatternMessage1 & XiPatternMessage2)	• Describes the message sent at runtime and references the data type used.
Data Type (XiPatternDataType1 & XiPatternDataType2)	• Describes the data structure of the message. The structure of data type XiPatternDataType2 is different to the structure of data type XiPatternDataType1 in the following ways: • In data type XiPatternDataType1, two separate elements are used to specify the person's first and second name, whereas in data type XiPatternDataType2, only one element is used (FullName). • In data type XiPatternDataType1, the name of the element that specifies the telephone number is TelephoneNumber, whereas in data type XiPatternDataType2, the name is PhoneNumber.
Operation Mapping (XiPatternInterface1ToInterface2)	• Describes the mapping between the source and target interface.
Message Mapping (XiPatternInterface1ToInterface2)	• Describes the mapping between the source and target structure in detail.

5.2 Configuring the Process Integration Scenario

To configure this Variant a new Integration Flow is created.

5.2.1 Creating the Integration Flow

Perform the following steps to create a new integration flow:

1. In the Process Integration Designer choose *New* > *Integration Flow (*  *)*.
2. In category Enterprise Integration Patterns select the *Recipient List* Pattern and set the name or the Integration Flow as *XiPatternSFTPScenario_Mapping.*
3. Choose Next.
4. As Sender Business System select the Business System <SID>_SFTP_PGP_BS1 you imported from SLD using the Browse button.
5. As Interface select XiPatternInterface1.
6. In Tab Receiver Systems as Receiver System select the Business System <SID>_ SFTP_PGP_BS2 using the input help for the Receiver Name.
7. As Receiver Interface select XiPatternInterface1.
8. Now add one more receiver using the add button and similarly assign Business System <SID>_ SFTP_PGP_BS3 & Interface XiPatternInterface2.
9. Choose Finish.
10. The integration Flow will be displayed in a graphical overview.

11. On the line representing the message flow to receiver <SID>_ SFTP_PGP_BS3 in the context menu select Add Mapping.

12. Select the mapping object in the graphical view. The properties tab will open.

13. Using the Browse functionality select the operation mapping XiPatternInterface1ToInterface2.

5.2.2 Creating Channels

You perform the following steps to configure the connection of the process integration scenario. You activate the relevant sender-receiver relation (between the sender and receiver component) and assign both the sender and receiver a (sender or receiver) communication channel.

1. In the graphical editor, double click on channel for the sender component. The Details tab for the channel will open.

2. As Channel Name set *Sender*.

In the application *NWA > Communication Channel Monitoring* the channels can be filtered based on the value of the field *Channel ID.* (This is generated by appending the “Integration Flow name” + “_” + “the Channel Name”). In the above case it will be - *XiPatternSFTPScenario_Mapping_Sender*.

3. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

4. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > SFTP Server	• Server	• The Host Name/ IP Address on which SFTP server is running
	• Port	• The SFTP server Port number. • By default **22** is set**. (It ’s the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific > Source > Proxy	• Proxy	• HTTP
	• Server	• The Host Name/ IP Address on which HTTP proxy is running
	• Port	• Port number
	• Username	• Leave it Blank
	• Password	• Leave it Blank
Adapter Specific > Source > Authentication	• Authentication Method	• Private Key
	• Username	• XIDEMO
	• Private key View	• SFTP_TEST (refer sec 2.3.1)
	• Private key Entry	• sftp_keystore (refer sec 2.3.1)
Adapter Specific > Source > File	• File Name	• XiPatternSenderFile?.*
	• Directory	• In this case of the sender communication channel, enter the

		whole path for the file directory *Variant03/Input*. Example: *~/<selected path>/SFTP&PGP /Variant03/Input*
Adapter Specific > Source > Period	• Poll Interval (min)	• 1
Adapter Specific > Processing > Processing Parameters	• Delete File	• No
	• Process Sequence	• Descending by date
Adapter Specific > Processing > Quality of Service	• Quality of Service	• Exactly once (asynchronous)
Adapter Specific > Advanced > Adapter Specific Message - Attributes	• Set adapter specific message attributes	• Yes • Check all the checkboxes –Directory; File Size; Timestamp and SFTP Host. (File Name is set by default)

5. Now go back to the Graphical editor by clicking on the button ().

6. In the graphical editor, now double click on channel for the receiver component - SID>_ SFTP_PGP_BS2. The Details tab for the channel will open.

7. As Channel Name set *Receiver1*.

8. As Adapter Type select SFTP of Software Component SFTP ADAPTER1.0

9. In tab Adapter- Specific fill the values as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > SFTP Server	• Server	• The Host Name/ IP Address on which SFTP server is running.
	• Port	• The SFTP server Port number. • By default **22** is set**. (It 's the TCP port which is used bySSH)**
	• Timeout(ms)	• 30000
	• Server Fingerprint	• The server finger print. (Refer section 2.3.3)
Adapter Specific > Source > Proxy	• Proxy	• HTTP
	• Server	• The Host Name/ IP Address on which HTTP proxy is running
	• Port	• Port number
	• Username	• XIDEMO
	• Password	• Password
Adapter Specific > Source > Authentication	• Authentication Method	• Private Key
	• Username	• XIDEMO
	• Private key View	• SFTP_TEST (refer sec 2.3.1)
	• Private key Entry	• sftp_keystore (refer sec 2.3.1)

Adapter Specific > Source > File	• File Name	• %FileName%
	• File Path	• In this case of the receiver communication channel, enter the whole path for the file directory *Variant03/Output1*. Example: *~/<selected path>/SFTP&PGP /Variant03/Output1*
	• Create Directory	• No
	• Overwrite	• No
Adapter Specific > Processing > Processing Parameters	• Add Timestamp to filename	• Yes
	• Add Message-ID to filename	• No
	• Write Mode	• Direct
Adapter Specific > Advanced > Adapter Specific Message - Attributes	• Use adapter specific message attributes	• Yes • File Name is set by default

10. Now go back to the Graphical editor by clicking on the button ( ).
11. Select the above configured channel in the graphical editor; in the context menu choose C*opy.*
12. Now select the channel connecting to the system <SID>_SFTP_PGP_BS3. In the context menu choose *Paste.* It will copy all the configurations done above.
13. Now double click on it and open the Details tab.
14. As Channel Name set *Receiver2*.
15. Now make the following changes in tab Adapter- Specific tab as mentioned in the table below:

UI Area	Field	Value
Adapter Specific > Source > Proxy	• Username	• Delete the username (make the field empty)
	• Password	• Delete the Password (make the field empty)
Adapter Specific > Source > Authentication	• Authentication Method	• Password
	• Username	• XIDEMO
	• Password	• Password
Adapter Specific > Source > File	• File Name	• XiPatternReceiverFile.txt
	• File Path	• In this case of the receiver communication channel, enter the whole path for the file directory *Variant03/Output2*. Example: *~/<selected path>/SFTP&PGP /Variant03/Output2*
	• Overwrite	• Yes
Adapter Specific >	• Add Timestamp to	• No

Processing > Processing Parameters	filename	
	• Write Mode	• Use temporary file
Adapter Specific > Advanced > Adapter Specific Message - Attributes	• Use adapter specific message attributes	• No

16. Now go back to the Graphical editor by clicking on the button ( ).

5.2.3 Defining the Routing conditions

In the following steps, you configure the routing conditions.

1. Select the element *Recipient List* to add the routing conditions. The properties tab for the receiver determination will open. Select the properties tab.

2. For the receiver component <SID>_SFTP_PGP_BS2 call the expression editor by selecting the line for the receiver and pressing Edit button.

3. In the condition editor press Ctrl + Space and select Xpath.

4. Add a “.” next to Xpath & hit Ctrl + Space again. The data structures of the message are displayed.

5. Select /p1:XiPatternMessage1/Person/CountryCode.

6. Choose the operator Equal To (=) in the Operators section via double click.

7. In the expression section enter “US”. The expression should now look like this:
   Xpath./p1:XiPatternMessage1/Person/CountryCode = "US"

8. Choose OK.

9. You have specified the routing condition CountryCode = US.

   

   At runtime, messages that have the value US entered for the element CountryCode are sent to receiver <SID>_SFTP_PGP_BS2.

10. Following this procedure, create the routing condition CountryCode = “DE” for the configured receiver <SID>_SFTP_PGP_BS3.

5.2.4 Saving, Activating & Deploying the Integration Flow

In the following steps, you save the integration flow with all its objects and activate it for the runtime.

1. Save the Integration Flow by pressing the save button ( ).

2. Use the Activate entry in the context menu of the integration flow *XiPatternSFTPScenario_Mapping* to activate the configuration.

3. Use the Deploy entry in the context menu of the integration flow *XiPatternSFTPScenario_Mapping* to deploy it in the runtime.

5.3 Executing the Use Case

You perform the following steps to check that the use case is executed without errors.

1. Open the configured directory *Input* under *~/SFTP&PGP/Variant03* on the SFTP server. (Refer section 2.4).

2. Rename the xml files to XiPatternSenderFile1.xml & XiPatternSenderFile3.xml.

3. Modify (change the Last or First name) the file XiPatternSenderFile3.xml. So that the time stamp is different from XiPatternSenderFile1.xml.

4. Once the sender channel finishes processing, check in the channel monitor (Configuration and Monitoring Home > Adapter Engine > Communication Channel Monitor) the file XiPatternSenderFile3.xml is processed first by the sender channel (as in the sender channel processing sequence is set –Descending by date). Then stop the sender channel.

5. Check whether the file has arrived in directory ~/Variant03/Output1. Its name will be same as the sender file XiPatternSenderFile1.xm + Time stamp. Open the file and check that the country code US is present in the personal data.

6. Check whether a file has arrived in directory ~/Variant03/Output2. Open the file and check that the country code DE is present. The structure will have changed:
    a) The first and the last name of the person have been concatenated.
    b) The field for the telephone number has a new name -PhoneNumber.

Furthermore, you can check the processing of the message in monitoring. To do this, proceed as follows:

1. Start the Monitoring by choosing Configuration and Monitoring Home on the Advanced Adapter Engine Extended start page.

2. Choose Message Overview.

3. Select Database.

4. Use appropriate filter criteria to restrict the number of XML messages displayed (for example, the processing period). On the very right hand side select Advanced to get all possible filter criteria displayed. To select using your *Integration Flow* name use the input help for Integration Scenario under the section *Message Header Data*, put in the Integration Flow name *XiPatternSFTPScenario_Mapping* into the value field, press enter and select your Integration Flow.

5. Choose Go.

6. The system displays the filtered messages in a table.

7. Select any one message then click on Open Message Button. The tab Message Attributes displays all the adapter specific message attributes along with the values (as set in the Sender channel Adapter Specific > Advanced > Adapter Specific Message –Attributes).

8. Start the channel XiPatternSFTPScenario_Mapping_Sender in the Configuration and Monitoring Home > Adapter Engine > Communication Channel Monitor.

9. Check the directory ~/Variant03/Output2. Still it should contain single file. As the file is overwritten. The time stamp of the file would have changed.

6 VARIANT04: ONE SENDER AND ONE RECEIVER WITH PGP MODULE

This variant enables you to configure a simple message exchange between one sender and one receiver using SFTP Adapter with the PGP Module.

Here, with the use of the PGP Module parameters the user is able to Compress/Decompress, Encrypt/Decrypt, Sign/Verify Signature, as well as set the format and ASCII armor for the message, configured in the Sender and Receiver Communication channels. No mapping is executed between the outbound and inbound interface in this variant.

Also, in this variant we configure the scenario with the SFTP Adapter features of SOCKS 5 proxy with Authentication (Password/Private Key based SSH server Authentication) and processing of a Duplicate File using the feature *Duplicate File Check*.

6.1 Summary of the Design Objects Used

Object type (Name)	Description
Service Interfaces (*XiPatternInterface2*)	Specifies the communication mode and references the message type used.
Message Type (*XiPattermMessage2*)	Describes the message sent at runtime and references the data type used.
Data Type (*XiPatternDataType2*)	Describes the data structure of the message.

6.2 Configuring the Integration Flow Scenario

In configuration, the communication components you defined earlier enable you to address the involved business systems as senders/receivers of messages from the Process Integration Designer.
You have already described the system landscape in the SLD. You perform the following configuration steps in the SAP Process Integration Designer.

6.2.1 Calling the Process Integration Designer

First, open the SAP NetWeaver Developer Studio.
Set the connection data for accessing the Integration Directory under the menu *Process Integration* → *Change Preferences*. The connection details to the System have to be maintained using URL or Host and Port.
To call the SAP Process Integration Designer follow the menu path *Window* → *Open Perspective* → *Other* → *SAP Process Integration Designer*.
Logon to the system using the Menu *Process Integration* → *Connect* providing your user credentials.

6.2.2 Creating the Integration Flow

Perform the following steps to configure the Integration Flow in SAP NetWeaver Developer Studio.

6. In the Main menu, select New-> Integration Flow.
7. In the Integration flow dialog box, choose *Enterprise Integration Patterns* category and *Point-to-Point Channel* pattern.
8. Enter the name of the Integration flow as `XiPatternSFTPScenario_PGP`. Choose Finish.

6.2.3 Assigning Communication Components and Interface

You perform the following steps to assign communication components to the application components of the integration flow scenario. You use the business system components that you created before (see 2.5).

1. In the Model Configurator, assign the Business system `<SID>_SFTP_PGP_BS4` to the sender system by selecting the Sender element -> right click -> Assign System.

2. Following the same procedure as while assigning the business system to the Sender component, assign `<SID>_SFTP_PGP_BS5` to the component Receiver.

3. Select the Sender Interface, right click and select Assign Interface. The dialog *Choose Interface* will open. Browse and select `XiPatternInterface2`.

4. Following the same procedure as while assigning the Sender Interface, assign the same interface `XiPatternInterface2` to the Receiver Interface.

6.2.4 Configuring the Communication channels

You perform the following steps to configure the connection in the Integration flow. You activate the relevant sender-receiver relation (between the sender and receiver component) and assign both the sender and receiver a (sender or receiver) communication channel.

1. In the graphical editor, right-click on channel for the sender component. Select *Configure Channel*. The Channel editor screen will open.
2. In the tab *General*, enter the name for the Sender communication channel as "Sender"*.* Under the block Adapter Type, browse for the Adapter Type *SFTP* (software component version *SFTP ADAPTER 1.0*, namespace *http://sap.com/xi/XI/SFTP*).
3. Now go to the *Adapter Specific* tab, and under the *Source* sub-tab enter the details according to the table below:

UI Block	Field	Value
SFTP Server	Server	Hostname (or IP Address) on which SFTP server is running
	Port	Port number on which SFTP Server is running (22 by default)
	Timeout(ms)	30000
	Fingerprint	Server fingerprint (Refer section 2.3.3)
Proxy	Proxy	SOCKS5
	Server	Hostname or (IP Address) on which SOCKS proxy is running
	Port	Port number corresponding to the SOCKS5 proxy
Authentication	Authentication Method	Private Key
	Username	*XIDEMO*
	Private Key View	SFTP_TEST (Refer Section 2.3.1)
	Private Key Entry	sftp_keystore (Refer Section 2.3.1)
File	Filename	*XiPatternSenderFile4.xml*
	Directory	Path to the Source Directory where the input file is stored (Refer Section 2.4) In this case enter the whole path for `Variant04/Input`. Example *~/<selected path>/SFTP&PGP /Variant04/Input*
Period	Poll Interval (min)	1

4. Now go to the *Processing* sub-tab, Uncheck the *Delete File* option and check the *Duplicate file checking* option.
5. Now go to the *Modules* tab, add the *Module Name* ‘‘localejbs/PGPEncryption’’ at *Processing Sequence* 1 by clicking on *Add* button. Give a *Module key* for the PGP Encryption Module as ‘‘pgpenc’’. And enter the Module Configuration as following:

Module Key	Module Parameter	Parameter Value
pgpenc	keyRootPath	Path to the location on the PI Server where the PGP certificates are stored (Refer Section 2.3.1)
	partnerPublicKey	<ReceiverPublicKeyName>.asc (Refer Section 2.3.1)
	ownPrivateKey	<SenderPrivateKeyName>.asc (Refer Section 2.3.1)
	pwdOwnPrivateKey	Passphrase for the Sender Private Key (Refer Section 2.3.1)
	applyEncryption	true
	encryptionAlgo	Encryption Algorithm, for example AES_128
	applySignature	true
	signingAlgo	Signing Algorithm, for example MD5
	applyCompression	Compression Algorithm, for example ZIP
	format	text
	asciiArmored	true

The Encryption Algorithms supported by the PGP Module are **AES_128, AES_192, AES_256, BLOWFISH, DES, 3DES, CAST5,** and **TWOFISH.**

The Signing Algorithms supported by the PGP Module are **MD5, RIPEMD160, SHA1, SHA224, SHA256, SHA384,** and **SHA512**.

The Compression Algorithms supported by the PGP Module are **ZIP, ZLIB,** and **BZIP2.**

Any of the mentioned Encryption/Signing/Compression Algorithms can be used while configuring the PGP Module in the Sender Communication channel.

6. Following the same procedure, configure the Receiver Communication channel.
7. In the tab *General*, enter the name for the Receiver communication channel as “Receiver’’. Under the block *Adapter Type*, browse for the Adapter Type *SFTP* (software component version *SFTP ADAPTER 1.0*, namespace *http://sap.com/xi/XI/SFTP*).

8. Now go to the *Adapter Specific* tab, and under the *Source* sub-tab enter the details according to the table below:

6.2.5 Saving and Activating the Integration Flow

In the following steps, you save the integration flow with all its objects and activate it for the runtime.

1. Save the Integration Flow by pressing the save button ().

2. Use the *Activate* entry in the context menu of the integration flow `XiPatternSFTPScenario_PGP` to activate the configuration.
3. Use the *Deploy* entry in the context menu of the integration flow `XiPatternSFTPScenario_PGP` to deploy it in the runtime.

6.2.6 Executing the Use Case

You perform the following steps to check that the use case is executed without errors.

1. Open the file directory *Output*. Remove all the files in this target folder.

2. Open the file Directory *Input* and rename the file *ZXiPatternSenderFile4.xml* as *XiPatternSenderFile4.xml.*

3. Execute the scenario and check that the file has arrived in the *Output* folder without any issues.
   Since it tests only the SOCKS 5 proxy connectivity, if the end to end transfer is successful, the test is considered to be successful.

4. Open the file and check whether the content has changed (compare with the original file X*iPatternSenderFile4.xml*).
   The file must not have been changed when this variant is executed.

5. Execute the scenario once again to check for the processing of Duplicate File.
   The File should not be processed the second time.

Check the processing of the message in the Channel Monitoring and Message Monitoring (**to verify the file transfer and PGP Module features**). To do this, proceed as follows:

Channel Monitoring:

1. Start the Monitoring by choosing *SAP Netweaver Administrator* on the Advanced Adapter Engine Extended start page.
2. Choose *SOA* → *Monitoring* → *Communication Channel Monitor*
3. Use appropriate filter criteria to restrict the number of channels displayed. On the very right hand side select *Advanced* to get all possible filter criteria displayed. To select your channels, put in the channel ID (you can find it in the channel editor screen) `XiPatternSFTPScenario_PGP*` into the communication channel field, press *Go* and select your sender channel from the list.
4. Check that the channel is running without error.
5. In the Processing Details section you can find the processing logs and the links to the processed messages. The link can be followed to get the message details.

Message Monitoring:

1. Start the Monitoring by choosing *SAP Netweaver Administrator* on the Advanced Adapter Engine Extended start page.
2. Choose *SOA* → *Monitoring* → *Communication Channel Monitor.*
3. Select *Database*.
4. Use appropriate filter criteria to restrict the number of XML messages displayed (for example, the processing period). On the very right hand side select *Advanced* to get all possible filter criteria displayed and open the Message Header Data section. To select using your Integration Flow name put in the name `XiPatternSFTPScenario_PGP` into the field Integration Flow.
5. Choose *Go*.

   The system displays the selected messages in a table. You want to locate the messages that were sent during execution.
6. Select the message to be displayed in the *Message List* block and go to the *Message Log* tab.

   Verify the following w.r.t the *PGP Module*:
   1. Message Format should be in ‘text’

2. Message should be ‘ASCII Armored’
3. Message should be compressed. (Algorithm ZIP)
4. Message should be encrypted with the Algorithm (AES_128)
5. Message should be Signed. (Algorithm MD5)

7. Select the message to be displayed by selecting the appropriate Message and then choose *Open Message*.

   The tab *Payloads* displays the message content for the various versions of the message during processing.
   The Message Content in this tab should be a wired message due to format/asciiArmor/encryption/signing/compression.

   The output file content in the target Directory should be in plain text/message after decryption/verification signature/de-compression.

7 VARIANT05: ONE SENDER AND ONE RECEIVER WITH PGP MODULE (DEFAULT AND INCORRECT VALUES FOR MODULE PARAMETERS)

This variant enables you to configure a simple message exchange between one sender and one receiver using SFTP Adapter with the PGP Module.
Here, we use the Default/Incorrect values for the Module parameters of the PGP Module.

Here, with the use of the PGP Module parameters allows the user to Compress/Decompress, Encrypt/Decrypt, Sign/Verify Signature, as well as set the format and ASCII armor for the message, configured in the Sender and Receiver Communication channels. No mapping is executed between the outbound and inbound interface in this variant.

Also, in this variant we configure the scenario with the SFTP Adapter features of SOCKS 5 proxy with Authentication (Password/Private Key based SSH server Authentication) and the *Internal Modification Check*.

7.1 Summary of the Design Objects Used

Object type (Name)	Description
Service Interfaces (*XiPatternInterface2*)	Specifies the communication mode and references the message type used.
Message Type (*XiPattermMessage2*)	Describes the message sent at runtime and references the data type used.
Data Type (*XiPatternDataType2*)	Describes the data structure of the message.

7.2 Configuring the Integration Flow Scenario

In configuration, the communication components you defined earlier enable you to address the involved business systems as senders/receivers of messages from the Process Integration Designer.
You have already described the system landscape in the SLD. You perform the following configuration steps in the SAP Process Integration Designer.

7.2.1 Calling the Process Integration Designer

First, open the SAP NetWeaver Developer Studio.
Set the connection data for accessing the Integration Directory under the menu *Process Integration → Change Preferences*. The connection details to the System have to be maintained using URL or Host and Port.
To call the SAP Process Integration Designer follow the menu path *Window → Open Perspective → Other → SAP Process Integration Designer*.
Logon to the system using the Menu *Process Integration → Connect* providing your user credentials.

7.2.2 Creating the Integration Flow

Perform the following steps to configure the Integration Flow in SAP NetWeaver Developer Studio.

1. In the Main menu, select New-> Integration Flow.
2. In the Integration flow dialog box, choose *Enterprise Integration Patterns* category and *Point-to-Point Channel* pattern.
3. Enter the name of the Integration flow as `XiPatternSFTPScenarioPGP_Def&Inc`. Choose Finish.

7.2.3 Assigning Communication Components and Interface

You perform the following steps to assign communication components to the application components of the integration flow scenario. You use the business system components that you created before (see 2.4).

1. In the Model Configurator, assign the Business system `<SID>_SFTP_PGP_BS6` to the sender system by selecting the Sender element -> right click -> Assign System.

2. Following the same procedure as while assigning the business system to the Sender component, assign `<SID>_SFTP_PGP_BS7` to the component Receiver.

3. Select the Sender Interface, right click and select Assign Interface. The dialog Choose Interface will open. Browse and select `XiPatternInterface2`.

4. Following the same procedure as while assigning the Sender Interface, assign the same interface to the `XiPatternInterface2` Receiver Interface.

7.2.4 Configuring the Communication channels

You perform the following steps to configure the connection in the Integration flow. You activate the relevant sender-receiver relation (between the sender and receiver component) and assign both the sender and receiver a (sender or receiver) communication channel.

1. In the graphical editor, right-click on channel for the sender component. Select *Configure Channel*. The Channel editor screen will open.
2. In the tab General, enter the name for the Sender communication channel as “Sender*”.* Under the block Adapter Type, browse for the Adapter Type *SFTP* (software component version *SFTP ADAPTER 1.0*, namespace *http://sap.com/xi/XI/SFTP*).
3. Now go to the *Adapter Specific* tab, and under the *Source* sub-tab enter the details according to the table below:

UI Block	Field	Value
SFTP Server	Server	Hostname (or IP Address) on which SFTP server is running
	Port	Port number on which SFTP Server is running (22 by default)
	Timeout(ms)	30000
	Fingerprint	Server fingerprint (Refer section 2.3.3)

Proxy	Proxy	SOCKS5
	Server	Hostname or (IP Address) on which SOCKS proxy is running
	Port	Port number corresponding to SOCKS5 proxy
	Username	*XIDEMO*
	Password	Password for the user
Authentication	Authentication Method	Password
	Username	*XIDEMO*
	Password	Password for the user
File	Filename	*XiPatternSenderFile4.xml*
	Directory	Source Directory in the SFTP server where the input file is stored (Refer Section 2.4) In this case enter the whole path for `Variant05/Input`. Example *~/<selected path>/SFTP&PGP /Variant05/Input*
Period	Poll Interval (min)	1

4. Now go to the *Processing* sub-tab, Uncheck the *Delete File* option and enter 30000 in the field *Internal Modification Check*.
5. Now go to the *Modules* tab, add the *Module Name* ‘‘localejbs/PGPEncryption’’ at *Processing Sequence* 1 by clicking on *Add* button. Give a *Module key* for the PGP Encryption Module as ‘‘pgpenc’’. And enter the Module Configuration as following:

Module Key	Module Parameter	Parameter Value
pgpenc	keyRootPath	Path to the location on the PI Server where the PGP certificates are stored (Refer Section 2.3.1)
	partnerPublicKey	<ReceiverPublicKeyName>.asc (Refer section 2.3.1)
	ownPrivateKey	<SenderPrivateKeyName>.asc (Refer section 2.3.1)
	pwdOwnPrivateKey	Passphrase for the Sender Private Key (Refer section 2.3.1)
	applyEncryption	true
	encryptionAlgo	INCORRECT
	applySignature	false
	applyCompression	INCORRECT
	format	INCORRECT
	asciiArmored	INCORRECT

The Encryption Algorithms supported by the PGP Module are **AES_128, AES_192, AES_256, BLOWFISH, DES, 3DES, CAST5,** and **TWOFISH.**

The Signing Algorithms supported by the PGP Module are **MD5, RIPEMD160, SHA1, SHA224, SHA256, SHA384,** and **SHA512**.

The Compression Algorithms supported by the PGP Module are **ZIP, ZLIB,** and **BZIP2.**

Any of the mentioned Encryption/Signing/Compression Algorithms can be used while configuring the PGP Module in the Sender Communication channel.

In this variant, the value INCORRECT is any incorrect value for the algorithms in which case the default algorithms/values are executed.

The Default algorithm for Encryption is **CAST5**, for Signing is **SHA1 a**nd that for Compression is **ZLIB**.

The Default value for format is **BINARY** and that for asciiArmored is **TRUE**.

6. Following the same procedure, configure the Receiver Communication channel.
7. In the tab General, enter the name for the Receiver communication channel as “Receiver’’. Under the block Adapter Type, browse for the Adapter Type *SFTP* (software component version *SFTP ADAPTER 1.0*, namespace *http://sap.com/xi/XI/SFTP*).

8. Now go to the *Adapter Specific* tab, and under the *Source* sub-tab enter the details according to the table below:

7.2.5 Saving and Activating the Integration Flow

In the following steps, you save the integration flow with all its objects and activate it for the runtime.

1. Save the Integration Flow by pressing the save button ().
2. Use the *Activate* entry in the context menu of the integration flow `XiPatternSFTPScenarioPGP_Def&Inc` to activate the configuration.
3. Use the *Deploy* entry in the context menu of the integration flow `XiPatternSFTPScenarioPGP_Def&Inc` to deploy it in the runtime.

7.2.6 Executing the Use Case

You perform the following steps to check that the use case is executed without errors.

1. Open the file directory *Output* using an SFTP client. Remove all the files in this target folder.

2. Open the file Directory *Input* and rename the file *ZXiPatternSenderFile4.xml* as *XiPatternSenderFile4.xml.*

3. Execute the scenario and check that the file has arrived in the *Output* folder without any issues.
   Since it tests only the SOCKS 5 proxy connectivity, if the end to end transfer is successful, the test is considered to be successful.

4. Open the file and check whether the content has changed (compare with the original file *XiPatternSenderFile4.xml*).
   The file must not have been changed when this variant is executed.

5. Now modify the Input file for this variant within 30 seconds (30000 ms) of the next poll as mentioned in the *Internal Modification Check* field in the Sender Communication channel.

The File should not be processed the next time (after modifying the file within the given time frame). If the input file is not modified within the time frame the file would be processed.

If there are more than one file present in the *Input* file directory and one of them is found modified the processing of the modified file is skipped and the other files are processed.

Check the processing of the message in the Channel Monitoring and Message Monitoring (**to verify the file transfer and PGP Module features**). To do this, proceed as follows:

Channel Monitoring:

1. Start the Monitoring by choosing *SAP Netweaver Administrator* on the Advanced Adapter Engine Extended start page.
2. Choose *SOA* → *Monitoring* → *Communication Channel Monitor*
3. Use appropriate filter criteria to restrict the number of channels displayed. On the very right hand side select *Advanced* to get all possible filter criteria displayed. To select your channels, put in the channel ID (you can find it in the channel editor screen) `XiPatternSFTPScenarioPGP_Def*` into the communication channel field, press *Go* and select your sender channel from the list.
4. Check that the channel is running without error.
5. In the Processing Details section you can find the processing logs and the links to the processed messages. The link can be followed to get the message details.

Message Monitoring:

1. Start the Monitoring by choosing *SAP Netweaver Administrator* on the Advanced Adapter Engine Extended start page.
2. Choose *SOA* → *Monitoring* → *Communication Channel Monitor.*
3. Select *Database*.
4. Use appropriate filter criteria to restrict the number of XML messages displayed (for example, the processing period). On the very right hand side select *Advanced* to get all possible filter criteria displayed and open the Message Header Data section. To select using your Integration Flow name put in the name `XiPatternSFTPScenarioPGP_Def&Inc` into the field Integration Flow.
5. Choose *Go*.

   The system displays the selected messages in a table. You want to locate the messages that were sent during execution.
6. Select the message to be displayed in the *Message List* block and go to the *Message Log* tab.

   Verify the following w.r.t the *PGP Module*:
   1. Message Format should be in the default format ‘binary’
   2. Message should be ‘ASCII Armored’ by default
   3. Message should be compressed with the default Algorithm (ZLIB)
   4. Message should be encrypted with the default Algorithm (CAST5)
   5. Message should not be Signed.

7. Select the message to be displayed by selecting the appropriate Message and then choose *Open Message*.

   The tab *Payloads* displays the message content for the various versions of the message during processing.
   The Message Content in this tab should be a wired message due to format/asciiArmor/encryption/signing/compression.

   The output file content in the target Directory should be in plain text/message after decryption/verification signature/de-compression.

You can also execute the scenario by changing the PGP Encryption Module parameter values configured in the Sender communication channel for this Integration flow to the following and check for the expected result:
applyEncryption – false
applySignature – true
applyCompression - none
format – binary
asciiArmored – false

Verify the following w.r.t the *PGP Module*:

1. Message Format should be in ‘binary’
2. Message should not be ‘ASCII Armored’
3. Message should not be Compressed.
4. Message should not be encrypted
5. Message should be signed with the default algorithm (SHA1).

www.sap.com