



Industry Cloud Solutions

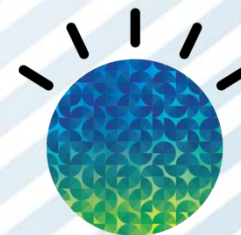
IBM
Software
Group

PGP Integration with Sterling B2B Integrator: Configuring, Troubleshooting and Best Practices

Ryan Wood – IBM Sterling B2b Integrator Support Engineer



© 2014 IBM Corporation



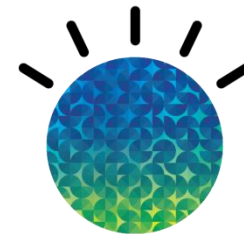
7/15/2014



Contact Information

- **Ryan Wood**
 - IBM Sterling B2B Integrator Support Engineer
 - woodry@us.ibm.com
 - Dublin, OH

- **Frank Bocinec**
 - IBM Sterling B2B Integrator Support Engineer
 - fbocinec@us.ibm.com
 - Dublin, OH



Agenda

- **Overview of Pretty Good Privacy (PGP)**
 - What is PGP?
 - High level process of setting up your PGP Server
- **Supported PGP Vendors**
 - Known limitations
 - Custom solutions
- **Integrating PGP with Sterling B2b Integrator (SBI)**
 - Components
 - PGP Adapters
 - Leveraging IBM Sterling FileGateway (SFG)
- **Troubleshooting**
 - Common Issues
 - Best Practices
- **Questions and Answers**



Overview of PGP

■ What is PGP?

- *Pretty Good Privacy* (PGP) is an open standard data encryption and decryption tool.
 - Provides cryptographic (secret or hidden) privacy for data communication in such a way that only authorized parties can read it.

■ Public Key / Conventional Cryptography

- Conventional – one key
- Public – pair of keys (more popular)
 - In order for others to verify your signature or encrypt data so that only you can decrypt it, they will need your public key.



■ Digital Signatures

- Serves purpose of a traditional “handwritten” signature, to verify the authenticity of the information's origin, and to provide “non-repudiation” or preventing sender from claiming the data was not sent.

For more information:

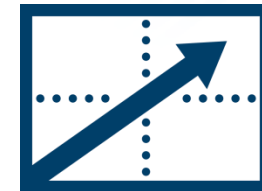
<http://www.pgpi.org/doc/pgpintro/>

<http://www.csee.umbc.edu/~woodcock/cm482/proj1/pgp.html>

PGP Server High Level Requirements

- 1) Install PGP Server
- 2) Create your key pair
- 3) Locate public/private key pair and important files

- - Protect your private key!
- -PGP Executable
- -PGP Path
- -Public Key Ring (pubring.pkr)
- -Secret Key ring (secring.skr)
- -Random No Seed (randseed.rnd)



4) Distribute your public key

-Partner will add key to their public keyring

In order for others to verify your signature or encrypt data so that only you can decrypt it, they will need your public key.

5) Obtain the public keys of others.

You need someone's public key to be able to encrypt data so that only they can decrypt it.

6) Verifying the public keys you get. Establish trust

For more information consult your PGP vendor's documentation

Supported PGP Environments

- **As of this publication the supported vendor list is as follows:**

- McAfee E-Business Server (version 8.1)
- McAfee E-Business Server (version 8.5)
- McAfee E-Business Server (version 8.5.1)
- McAfee E-Business Server (version 8.6)
- PGP® Command Line Freeware (version 6.5.8)
- PGP® Command Line (version 9.5) - PGP Corporation
- PGP® Command Line (version 9.8) - PGP Corporation
- PGP® Command Line (version 10.1) - PGP Corporation

- **Known issues**

- Symantec 10.3
- <http://www-01.ibm.com/support/docview.wss?uid=swg21636697>
- McAfee

- **Custom solutions**

- Command Line Adapter 2 process

- **RFE (Request for Enhancement) Community**

- <http://www.ibm.com/developerworks/rfe/b2bcommerce>



Integrating PGP with Sterling B2b Integrator

- **Components**
 - **PGP Server Manager**
 - The PGP Server Manager enables you to add, edit, and delete PGP servers
 - Secret Key Map Information
 - Key Name, ID, passphrase
 - Used for signing and decryption
 - **PGP Sponsor (optional)**
 - Command Line Adapter parameters
 - **PGP Partner (optional)**
 - Partner specific parameters using PGP Partner Manager.
- While executing a BP, you can associate a partner with an existing sponsor or server profile or both.

PGP Server Manager

PGP Server Profile

Name:

PGP Type

- McAfee E-Business Server (version 8.6)
- McAfee E-Business Server (version 8.5.1)
- McAfee E-Business Server (version 8.5)
- McAfee E-Business Server (version 8.1)
- PGP Command Line - Freeware (version 6.5.8)
- PGP® Command Line (version 9.5) - PGP Corporation
- PGP® Command Line (version 9.8) - PGP Corporation
- PGP® Command Line (version 10.1) - PGP Corporation

PGP Executable:

PGP Path:

PGP Public Key Ring:

PGP Secret Key Ring:

PGP Random No. Seed:

Unmasking the PGP Package and Unpackage Service

- **PGP Package/Unpackage is a “glorified” CLA2**
 - Stdout is the input we receive from the PGP Server
 - Stderr returns errors to the CLA2 configuration
 - Commands are tailored based on the Vendor selected in PGP Server Manager
 - Example:

```
C:\PGPcmdIn\PGP +pubring="C:\PGP\pubring.pkr" +secring="C:\PGP\secring.skr"  
+randseed="C:\Windows\randseed.rnd" +force +batchmode +armor=on +textmode=off +PGP_MIME=off -se  
InputFile.txt "sfglinux" -u sfgwin@sfg.com -z "password" -o InputFile.txt.asc
```

- These same commands can be found in the Vendors documentation for integrating PGP
- **Various Options on the PGP Package/Unpackage Service**
 - Questions to consider
 - Do I need to Sign AND Encrypt or simply Encrypt?
 - What is needed in both scenarios?
 - Will I be receiving encrypted documents that I will need Decrypt? If so what information is needed for the PGP Unpackage from my trading partner?

PGP Package Service

The screenshot displays the IBM Business Process Manager (BPM) interface. At the top, a process flow is visible: Start → PGP Package Service → End. Below this, the Service Editor for the PGP Package Service is shown. The configuration includes the following details:

- Name: PGP Package Service
- Config.: PGPPackageService
- Message To Service: Message From Service
- Output Msg: Obtain Process Data first, then Messages
- Message Name: PGPPackageServiceTypeInputMessage

A table of properties is displayed below the configuration:

Name	Value
ascii_armor	On
clearsig	
cmdline2svcname	
compress	On
conv_cipher	
conv_keymap_name	
discard_paths	
DocumentId	
info	Normal
inputFileNamePkg	
outputfilename	
pgp_partner_name	
pgp_sponsor_name	
pgparchive	
profile_name	
public_user	sfglinux
remoteName	
remotePort	
sda	
secret_keymap_name	sfgwin
setSoTimeout	
target_platform	
textmode	Off
tmpDir	
workingDir	

- In this example there is need to Encrypt AND Sign
- A secret key is required to make a signature.
- Recipients' public key(s) will be used to encrypt.
- The Partner (recipient) is *public_user* (sfglinux)
- The *secret_keymap_name* is your own key (sfgwin)
- Note conventional keymap is not needed if using public key cryptography

PGP Package Sample BPML

```
<process name="RW_PGP_Encrypt">
  <sequence name="optional">
    <operation name="One">
      <participant name="PGPPackageService"/>
      <output message="Xout">
        <assign to="." from="*"></assign>
        <assign to="profile_name">AFTPGPProfile</assign>
        <assign to="compress">on</assign>
        <assign to="secret_keymap_name">sfgwin</assign>
        <assign to="public_user">sfglinux</assign>
      </output>
      <input message="Xin">
        <assign to="." from="*"></assign>
      </input>
    </operation>
    <operation name="Release Service">
      <participant name="ReleaseService"/>
      <output message="ReleaseServiceTypeInputMessage">
        <assign to="." from="*"></assign>
        <assign to="TARGET">PrimaryDocument</assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
</process>
```

```
<assign to="PrimaryDocument"
from="//Document/@SCIObjctID"></assign>
  <operation name="File System Adapter">
    <participant name="AS3FSAdapter"/>
    <output message="FileSystemInputMessage">
      <assign to="." from="*"></assign>
      <assign to="Action">FS_EXTRACT</assign>
      <assign to="collectionFolder">C:\pgp</assign>
      <assign to="deleteAfterCollect">>false</assign>
      <assign to="extractionFolder">c:\pgp</assign>
    </output>
    <input message="inmsg">
      <assign to="." from="*"></assign>
    </input>
  </operation>
</sequence>
</process>
```

The PGP Package service does not make the encrypted document "PrimaryDocument", this BPML places the encrypted document into "PrimaryDocument" and writes it out to disk

PGP Package Sample

Execute Business Process

Name: RW_PGP_Encrypt Instance ID: 260291 User: admin

Completed
Status: Success

Step	Service	Status	Advanced Status	Started	Ended	Execution Node	Status Report	Document	Instance Data
4	AS3 FileSystem Adapter	Success	None	07/08/2014 3:47:29 PM EDT	07/08/2014 3:47:29 PM EDT	node1 [-]	Info	Info	Info
3	Assign Service	Success	None	07/08/2014 3:47:29 PM EDT	07/08/2014 3:47:29 PM EDT	node1 [-]	None	Info	Info
2	Release Service	Success	None	07/08/2014 3:47:29 PM EDT	07/08/2014 3:47:29 PM EDT	node1 [-]	None	Info	Info
1	PGP Package Service	Success	0	07/08/2014 3:47:29 PM EDT	07/08/2014 3:47:29 PM EDT	node1 [-]	Info	Info	Info
0	INITIATING_CONTEXT from user 'admin'	Success	None	07/08/2014 3:47:29 PM EDT	07/08/2014 3:47:29 PM EDT	node1 [-]	None	Info	Info

Primary Document

Process Name: RW_PGP_Encrypt Instance ID: 260291

Service Name: INITIATING_CONTEXT from user 'admin'

Document Name: clear_text_to_be_encrypted.txt Document Store: Database

Document ID: 945334147177f8635node1

Document in process data:

Test Input File - Clear Text to be Encrypted

Document

Process Name: RW_PGP_Encrypt Instance ID: 260291

Service Name: PGPPackageService

Document Name: clear_text_to_be_encrypted.txt Document Store: Database

Document ID: 715347147177f8635node1

Document in process data:

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8
```

```
hQCMA9KQvg2E5hLFAQP+LrE8Aia0Wz6UOCzC4SggxgeceKdqYSkIs/yvSR8UPRRn
mcnxAp/N/kLNB7Xo2DJ3WQtuXoGYC7pJzH+ImslzwKAGcTaKCbzw5w7Km9S2hov
LSyqxZhsCr9KYtiydIeEjvGkWuqyVlHuGgT90KfSGzbEvg1Dunz4Bx/xcIAaVyk
9oMboaRoFeGEQ8n+WNbmrD82uTX1BwYcS/gaJiIx0FI7I/97AAXF61hNqnBUx1kS
OM0x9BkmjDeNMq4HCZm6tgTrpqrxoE2UEvT7+DLIbtGuFO6TU8eOY4v0fyDr8UAE
bwKjWBBaT/Jq2/wpNLseMUup5CBQYApBSxXqmKTvg2EjRW5pxM/y+nY5vZvtZdUn
pp4t2Cq4kLqJTgMKT0E89cMMBtpPyiKQuXlGd0x1A71mT2Q0akpZiA3KPO5H+09v
roSe6LKEVsbAkn5c6JTiUzp3D8dVSBYICIXVd+ukNBOGeek1AZ2KJB/3JiIQBTp
tud791blyQ==
=Ymoa
```

```
-----END PGP MESSAGE-----
```

Execute Business Process

Name: RW_PGP_Encrypt Instance ID: 260291 User: admin

Status Report:

```
stdout=
A secret key is required to make a signature.
```

```
Recipients' public key(s) will be used to encrypt.
```

```
Passphrase is good
```

```
Key for user ID: sfglinux <sfglinux@sfg.com>
1024-bit RSA key, Key ID 0x84E612C5, created 2013/05/24
```

```
Transport armor file: clear_text_to_be_encrypted.txt.asc
```

```
stderr=Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSAREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.
```

PGP Unpackage Service

The screenshot displays the IBM Business Process Manager (BPM) interface. At the top, a process flow diagram shows a sequence: Start → PGP Unpackage Service → End. The PGP Unpackage Service is highlighted with a blue box. Below the diagram, the Service Editor for the PGP Unpackage Service is shown. It includes fields for Name (PGP Unpackage Service), Config (PGPUnpackageService), and Message Name (PGPUnpackageServiceTypeInputMessage). A table lists various parameters and their values.

Name	Value
cmdline2svcname	
conv_keymap_name	
DocumentId	
info	Normal
outputfilename	
pgp_partner_name	
pgp_sponsor_name	
profile_name	AFTPGPPProfile
remoteName	
remotePort	
secret_keymap_name	sfgwin
setSoTimeout	
signed_by	
tmpDir	
workingDir	

- In this example all that is needed is your **secret key map**
- In this example it is assumed that a file that was **signed** and **encrypted** from my partner (sfglinux) is ready to be run through this BP and be decrypted.
- The partners key (sfglinux) was already checked into my key map, within the PGP Server software outside of SBI.

PGP Unpackage Sample BPML

```

<process name="RW_PGP_Decrypt">
<sequence name="optional">
<operation name="One">
<participant name="PGPUnpackageService"/>
<output message="Xout">
<assign to="." from="*"></assign>
<assign to="profile_name">AFTPGPPProfile</assign>
<assign to="secret_keymap_name">sfgwin</assign>
</output>
  <input message="Xin">
    <assign to="." from="*"></assign>
  </input>
</operation>
</sequence>
</process>

```

Administration - Google Chrome
9.55.52.87:52000/ws/Tracker

Name: RW_PGP_Decrypt Instance ID: 260187 User: admin
Completed
Status: Success

Step	Service	Status	Advanced Status	Started	Ended	Execution Node	Status Report	Document	Instance Data
1	PGP Unpackage Service	Success	0	07/08/2014 3:21:17 PM EDT	07/08/2014 3:21:17 PM EDT	node1 [-]	Info	Info	Info
0	INITIATING_CONTEXT from user 'admin'	Success	None	07/08/2014 3:21:17 PM EDT	07/08/2014 3:21:17 PM EDT	node1 [-]	None	Info	Info

* Inline Invocation

Administration - Google Chrome
9.55.52.87:52000/ws/Tracker?action=getstatus&next=page.wfctrackerinfo&wfd_id=1329&workflow_id=2

CLOSE

▶ Execute Business Process

Name: RW_PGP_Decrypt Instance ID: 260187 User: admin
Status Report:

```

stdout=File is encrypted. Secret key is required to read it.

Key for user ID: sfgwin <sfgwin@sfg.com>
1024-bit RSA key, Key ID 0xC852B82F, created 2013/05/24
Key can sign.
Good signature from user "sfglinux <sfglinux@sfg.com>".
Signature made 2013/10/01 14:19 GMT

Plaintext filename: windows.txt.pgp.asc

stderr=Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSAREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

```

Leveraging PGP with IBM Sterling FileGateway (SFG)

- PGP encryption is supported by Sterling File Gateway, in combination with FTP and other protocols
- **Basic Steps to Implement**
 1. Create a Community
 - PGP Profile in SBI must be created first and must be named AFTPGPProfile
 2. Create Partner Profiles
 - Partners that send files into Sterling File Gateway are referred to as producers, and those that retrieve files are referred to as consumers. A partner can be a producer, a consumer, or both from an operational standpoint.
 3. Create a Routing Channel Template
 - Routing channel templates use file layer types to describe producer and consumer file structures
 4. Create Routing Channel
 - Link the template to a producer and consumer

IBM Sterling File Gateway: Create Community

- The PGP Server configuration in SBI **must** be named AFTPGPProfile for the keys to show up in the community dialogue boxes
- **Secret key for PGP signing**
 - Required if any of the consuming partners belonging to this community require PGP signed data
- **Secret key for PGP decryption**
 - Required if any of the producing partners belonging to this community send PGP encrypted data to the Router. This secret key may be the same or different from the one for PGP signing



Edit RW_PGP: Profile

Community Information

*Community Name: RW_PGP

Secret key for PGP signing: sfgwin ▼

Secret key for PGP decryption: sfgwin ▼

Cancel Finish

IBM Sterling File Gateway: Create Partner Profiles (1 of 2)

- In this example the Producer (sfgwin) is dropping off a clear text document, thus, PGP is options are not presented.
- The settings for the producer are independent of the settings for the consumers. If the producer is set to **Encryption**, regardless of whether the consumer is or is not, **only** encrypted files can be sent by the producer. If the producer is set to **No Encryption**, and the consumer is set to Encryption, unencrypted files are sent by the producer and the Router encrypts them before sending to the consumer.

Edit Partner: sfgwin

Profile	
Partner Name:	sfgwin
Partner Code:	sfgwin
Address:	4600 Lakehurst Ct Dublin, OH 43231 (800) IBM-SERV sfgwin@us.ibm.com
Phone:	
Email Address:	
 edit	
User Account	
User Name:	sfgwin
Authentication Type:	Local
Session Timeout (min):	15
Given Name:	sfg
Surname:	win
 edit	
Protocol	
Partner Role:	Producer of Data
Will sfgwin use either SSH/SFTP or SSH/SCP protocol to initiate connections?	No
 edit	
Community Membership	
Community Name:	RW_PGP
Joined Date:	2013-05-28 13:25:29.0
	

PGP Settings


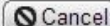
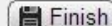
PGP Settings

When sfgwin sends PGP packaged files

... the files are processed in accordance with the Routing Channels (and their templates) that sfgwin is a producer for.

Note:




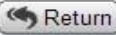
- * If sfgwin sends data that is encrypted, it will be decrypted using the Router's secret PGP key.
- * If sfgwin sends data that is signed, it will be verified using sfgwin's public PGP key if that key is present in the public key ring.

IBM Sterling File Gateway: Create Partner Profiles (2 of 2)

- In this example “sfglinux” is the Consumer
- In this scenario the Consumer is using FTP Protocol to receive the PGP encrypted document(s) from SFG
- For consumers, you specify in the Create Partner wizard that messages sent to the consumer must be encrypted, signed, or both. The PGP options of compression, text mode and ASCII armor can also be specified for each consumer.

Edit Partner: sfglinux

Profile	
Partner Name:	sfglinux
Partner Code:	sfglinux
Address:	123 Main Street Columbus, OH 43231
Phone:	(800) IBM-SERV
Email Address:	sfglinux@sfg.com
 edit	
User Account	
User Name:	sfglinux
Authentication Type:	Local
Session Timeout (min):	15
Given Name:	sfg
Surname:	linux
 edit	
Protocol	
Partner Role:	Consumer of Data
Connection Direction:	Listen Connection
Transport Method:	FTP
Connection Type :	active
FTP Server Host Name(or IP address):	oxnard
FTP Listen Port:	23532
User Name:	admin
Password:	*****
Base Directory:	/
Local Port Range:	
Control Port Range:	
Number of retries:	3
Interval between retries (in minutes):	1
FTP rename file:	no
Does sfglinux require data to be signed by the Router:	yes
Does sfglinux require data to be encrypted by the Router :	yes
Does sfglinux require data to be compressed by the Router:	no
Ascii Armor	on
Text Mode	off
 edit	
Community Membership	
Community Name:	RW_PGP
Joined Date:	2013-05-28 13:28:11.0
	

IBM Sterling File Gateway: Create Partner Profiles (2 of 2) Cont.

- PGP options of compression, text mode and ASCII armor can be specified for each consumer
 - ASCII armor involves encasing encrypted messaging in ASCII. Changes extension to .asc (**default On**)
 - Text mode passes the “Text Mode” flag to the PGP Server (**default Off**)

PGP Settings

PGP Settings

Does sfglinux require data to be signed by the Router

Yes No

Does sfglinux require data to be encrypted by the Router

Yes No

Please provide sfglinux's key id in the public key ring to be used for encryption

Does sfglinux require data to be compressed by the Router

Yes No

Ascii Armor Text Mode

Routing Channel Template – Encrypt and Sign

Routing Channel Template:

Template Name: PGP_Encrypt_Sign

Consumer Identification: Not Dynamic

Special Character Handling: No special character handling is specified

Provisioning Fact List:

Group Permissions:

Producer Group: All Partners

Consumer Group: All Partners

Producer Mailbox Path: /\${ProducerName}

Producer File Structures:

Producer File Structure: Unknown{.+}

Layer: Unknown

File name pattern as regular expression: .+

File name pattern group fact names, comma delimited:

Delivery Channel Templates:

Delivery Channel Template:

Consumer Mailbox Path: /\${ConsumerName}/Inbox

Consumer Mailbox: Not created at runtime

Consumer Protocol: protocol or mailbox

Consumer File Structure: PGP Encryption[\${ProducerFileName}_\${tYmdHMSL:RoutingTimestamp}]/Unknown[\${ProducerFileName}]

Layer: PGP Encryption

File name format: \${ProducerFileName}_\${tYmdHMSL:RoutingTimestamp}

Encryption Required: yes

Signature Required: yes

Layer: Unknown

File name format: \${ProducerFileName}

- In this Template the Producer file layer is “Unknown” as the partner could send any file format

- The file being sent to the Consumer is the PGP Encryption Layer
 - Outer layer for the Consumer must be encrypted and signed

- Inner file layer can be anything and in this example it is “Unknown”

Routing Channel Link

IBM Sterling File Gateway Welcome fg_sysadmin

Routes Participants Tools

Template : Producer : Consumer :

The number of Route Channels found: 1

Template	Producer ^	Consumer	Producer Mailbox Path
PGP_Encrypt_Sign	sfgwin	sfglinux	/sfgwin

- **Routing Channel Template may be Static or Dynamic**
 - **In this example Producer and Consumer is Static and defined**

Business Processes Executed Behind the Scenes of SFG

Monitor

Items 1-8 of 8

Status	ID	Name	State	Started	Ended	Deadline	Parent/Child	Expires
	293258	FileGatewaySendMessage	Completed	07/14/2014 1:58:51 PM	07/14/2014 1:58:54 PM	None	▲	
	293257	FileGatewayRoutePGPPackageDocument	Completed	07/14/2014 1:58:50 PM	07/14/2014 1:58:51 PM	None	▲	
	293256	FileGatewayMailboxRouteArrivedFile	Completed	07/14/2014 1:58:50 PM	07/14/2014 1:58:51 PM	None	▲ ▼	
	293254	FileGatewayMailboxRoute	Completed	07/14/2014 1:58:50 PM	07/14/2014 1:58:50 PM	None	▼	

Name: FileGatewayRoutePGPPackageDocument Instance ID: 293257 Service Name: PGP Package Service

Status Report:

```

stdout=
A secret key is required to make a signature.

Recipients' public key(s) will be used to encrypt.

Passphrase is good

Key for user ID: sfglinux <sfglinux@sfg.com>
1024-bit RSA key, Key ID 0x84E612C5, created 2013/05/24

Transport armor file: F:\SI52_ORA11G_52000\install\wd_Thread-30_1405360730908\clear_text_to_be_encrypted.txt.asc

stderr=Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSAREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.
    
```

Business Process Detail

Name: FileGatewayRoutePGPPackageDocument Instance ID: 293257 Status: Success State: Completed User: admin
 Deadline: None Contract ID: None

Action:

Steps 1-4 of 4

Step	Service	Status	Advanced Status	Started	Ended	Execution Node	Status Report	Document	Instance Data
0	Launched by File Gateway	Success	None	07/14/2014 1:58:50 PM	07/14/2014 1:58:50 PM	node1 [-]	None	info	info
1	Decision Engine Service	Success	2	07/14/2014 1:58:50 PM	07/14/2014 1:58:50 PM	node1 [-]	None	info	info
2	PGP Package Service	Success	0	07/14/2014 1:58:50 PM	07/14/2014 1:58:51 PM	node1 [-]	info	info	info
3	Assign Service	Success	None	07/14/2014 1:58:51 PM	07/14/2014 1:58:51 PM	node1 [-]	None	info	info

Document

Process Name: FileGatewayRoutePGPPackageDocument Instance ID: 293257

Service Name: PGP Package Service

Document Name: clear_text_to_be_encrypted.txt Document Store: Database

Document ID: 37941214735fe6d68node1

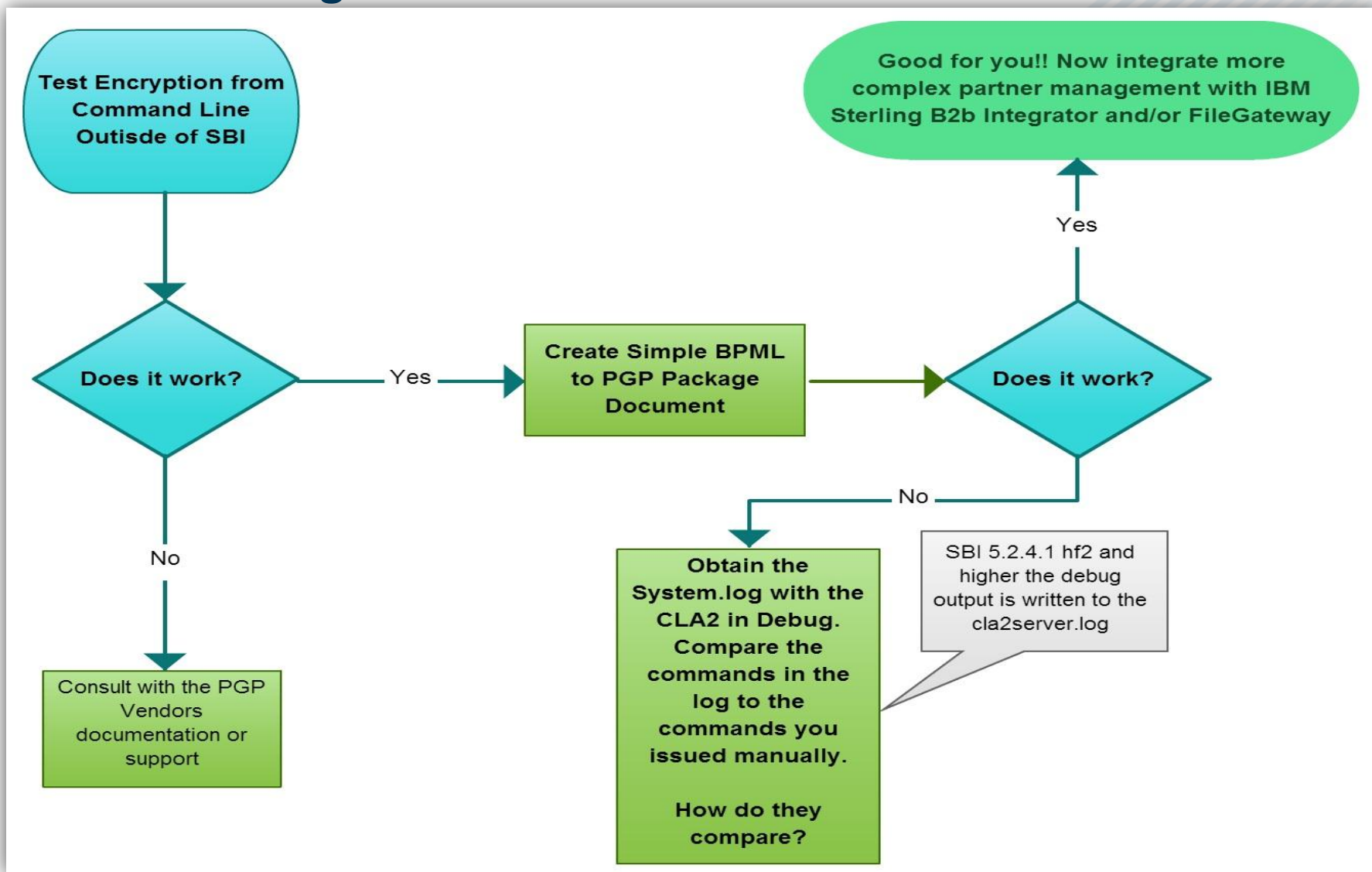
Document in process data:

```

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8

hQCMa9KQvg2E5hLFAQP/aBRr93dw9p2TFghbOKULQiBZd6FbaJq3uXA03d5d2Kyx
pbwK87tDML2bayjfnYcBYo1xJdAZTKCrq/KzYx9KzviCGhLx75IAv5HNOFWl1az
gLn3coUBqe8Y4m5Rc7kmTE7GsTGK6SviP8f1zvFjpwSB37BEKjP0zGR14xqNcjak
9RwZxNylJexZrEBkeZqc64ID7tVhQEfIghH5fHwXQEKZapOOnERfFEQeWp6nCR3t
uXPGZDExSVtyt7iCMzbnY4boh/0o02vaBu2PcX1BBPBA+dfEvgF4rcxUXILNSy3
5aI7qvhYaIjs41RL9h95tkGBLy8hS0dpnBEWqb4Jp8aB3kdKjQoUd9Du64wYLLt
t3VnG6DhJZf5b90D1rTy8d05puRig8j4K7JNuDsYnyhhaWfzi/YYYPna62XIMhh
wnS1ukzb/qgmeJte2KQt0Hzh4Rus02E7JEBPhzQddrs95EhS2zjmdUvbk8p8JGLJ
Hm85+1PA
=iUc/
-----END PGP MESSAGE-----
    
```

Troubleshooting



Common Issues and Best Practices

■ Problem description

- Attempts to encrypt a file via PGP within a routing channel template fail with the same message.
 - Exception in CmdLine2Thread
 - Expected file to collect does not exist: `/opt/app/install/wd_Thread-12_1403613511736/FILE_INVOICE_MMDDYYYY.txt.asc`
 - `stderr=Error: no application data directory found`

■ Resolution

- Permissions with the CLA2. CLA2 starts as ROOT and as such did not have the correct rights to create sub-directories or files locally.
- **Best Practice:** Created a new CLA2 Server, as a test, with a user with known set of permissions. Execute test - success.
 - Verify user in which SBI runs under has read/write/execute permissions to the PGP Path specified in the PGP Server Manager
 - “Expected file to collect does not exist:” – check permissions and working directories. Obtain full output from system or `cla2Server.log`

Common Issues and Best Practices

- **Problem Description:**
- PGP takes very long time to complete. Some BP instances have "Read timeout" error.
 - Socket Timeout value adjusted, slowness still observed
 - Customer ran pgp commands manually from the OS command line, same slowness observed
 - Narrowed the issue as not being SBI.
- **Resolution**
 - **Cluster Best Practice:** Work directories for PGP were on NFS-mounted file systems. Also, the PGP install and its pubring, secring, and randseed were on a share. Localized all these PGP elements and have not only dramatically increased our throughput, SBI is working as well. Customer increased local disk space for each node for work directories, and worked out a process to update key rings in two places rather than one as new keys arrive (in an automated fashion)

Common Issues and Best Practices

- **Best Practice: Adjust Socket Timeout**
 - **Add Parameter – `setSoTimeout` – PGPPackage/Unpackage Service**
 - `<assign to="setSoTimeout">120000</assign>`
 - Specifies, in milliseconds, how long the socket will wait in receive mode without receiving anything before timing out. This is necessary to ensure that a process doesn't "hang" indefinitely. Optional. Valid value: any integer. Default is 60000 milliseconds (60 seconds). If your command line process is going to take longer than the default 60 seconds to process completely, then increase this value accordingly.
- **File Gateway PGP Socket Timeout Setting**
 - `filegateway.properties`

```
##### Property: fgRoutePGPCmdLineSocketTimeout #####  
# Timeout value, in milliseconds for PGP package and unpackage operations invoked by Filegateway  
#  
fgRoutePGPCmdLineSocketTimeout=240000
```

Common Issues and Best Practices

■ Problem Description

■ Recently upgraded SBI from 5.x to 5.2.4.2 and PGP is no longer working

- Error \$ java.io.IOException: CmdLine2RemoteImpl.run: **Not starting CmdLine2 Server**. Was unable to load property file null from java - DcmdlineProps2=<Path>/CmdLine2server.properties or null at com.sterlingcommerce.woodstock.services.cmdline2.CmdLine2RemoteImpl.run(CmdLine2RemoteImpl.java:530) at
 - This is how we are invoking the Remote CIA2
 - /app/install/jdk/bin/java -jar /app/install/client/cmdline2/CLA2Client.jar 1567 > nohup.out &

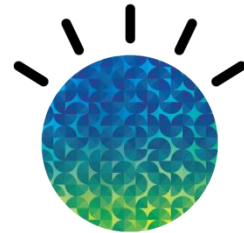
■ Resolution

- 5.2.4.1 Interim Fix 2 (and higher) introduced a **new** Command Line Adapter 2 (CLA2). For remote installations of the CLA2 it is necessary to re-deploy the adapter using the new bundle format
 - Note for the “local’ CLA2 , the CLA2 that runs out of the box on <baseport>+52, it will no longer start up automatically. You much add the following flag in the <si-install>/properties/sandbox.cfg , and run <si-install>/bin/setupfiles.sh for the CLA2 to start up as it did prior to upgrade.
 - **LAUNCH_CLA2_SERVER=true**

For more information on the above changes please refer to following documentation links

http://www01.ibm.com/support/knowledgecenter/SS3JSW_5.2.0/com.ibm.help.svcs_adpts_a_l.doc/Command_Line_adapter_2_5241_2.html?lang=en
http://public.dhe.ibm.com/software/commerce/doc/sb2bi/v5r2/SI5241_2_Upgrade_Impacts_CLA2.pdf

Poll



Questions and Answers

