Standard Operating Procedure (SOP)
PGP Encryption and Decryption Setup in Altova FlowForce Server

Table of Contents

Version: 1.1
Prepared By: [Your Name]
Date: [Insert Date]
Approved By: [Approver Name]

---

1. Purpose

This SOP provides detailed steps to set up and configure PGP encryption and decryption in **Altova FlowForce Server** on a Windows environment. It ensures secure file exchanges with partners by automating inbound file decryption and outbound file encryption.

---

2. Scope

This document applies to: - FlowForce administrators managing automated EDI/file workflows. - Operations teams handling partner onboarding and file exchange. - Security teams managing encryption keys.

---

3. Prerequisites

- **Altova FlowForce Server** installed and running on Windows.
- **Administrative access** to the FlowForce Server.
- **GnuPG (Gpg4win)** installed and available in PATH.
- **Service account** for FlowForce execution (example: `FLOWFORCE_USER`).
- Partner's **public PGP key** and your own **private PGP key**.

---

4. Directory Structure

Recommended folder layout:

```
C:\FlowForce\PGP\
   incoming\Encrypted-Incoming\   (incoming .pgp files)
   incoming\Decrypted-Out\       (decrypted files)
   incoming\Processed\           (successfully processed)
   incoming\Failed\              (failed decryption)
   outgoing\Plain\               (plain files to encrypt)
   outgoing\Encrypted\           (encrypted .pgp files)
   keys\                         (keys & passphrases, restricted access)
   scripts\                      (batch/powershell scripts)
   logs\                         (execution logs)
```

Apply strict **ACL permissions** to `keys` directory to ensure only `FLOWFORCE_USER` can access it.

---

5. GPG Installation & Verification

1. Download and install **Gpg4win**.
2. Verify installation:

   ```
   gpg --version
   ```

3. Confirm `gpg.exe` is accessible from the FlowForce environment.

---

6. Key Management

6.1 Generate New Key Pair

```
gpg --full-generate-key
```

- Key Type: RSA and RSA
- Key Size: 4096 bits
- Expiration: per policy (e.g., 1 year)
- Identity: `FlowForce-Prod`

6.2 Export Public Key

```
gpg --armor --export "FlowForce-Prod" > C:\FlowForce\PGP\keys\FlowForce-Prod-public.asc
```

Share this public key securely with the partner.

6.3 Import Partner Key

```
gpg --import C:\FlowForce\PGP\keys\partner-public.asc
```

Verify fingerprint and trust level:

```
gpg --fingerprint "Partner Name"
gpg --edit-key "Partner Name" trust quit
```

---

7. Passphrase Handling

- **Preferred:** Configure `gpg-agent` to cache the passphrase.
- **Alternative:** Use a passphrase file with restricted permissions:

  ```
  echo MySecurePassphrase > C:\FlowForce\PGP\keys\gpg-pass.txt
  icacls C:\FlowForce\PGP\keys\gpg-pass.txt /inheritance:r
  icacls C:\FlowForce\PGP\keys\gpg-pass.txt /grant:r "FLOWFORCE_USER:R"
  ```

8. Automation Scripts

8.1 Decryption Script (decrypt_all.bat)

```
@echo off
setlocal enabledelayedexpansion
SET INDIR=C:\FlowForce\PGP\incoming\Encrypted-Incoming
SET OUTDIR=C:\FlowForce\PGP\incoming\Decrypted-Out
SET PROCDIR=C:\FlowForce\PGP\incoming\Processed
SET FAILDIR=C:\FlowForce\PGP\incoming\Failed
SET PASSFILE=C:\FlowForce\PGP\keys\gpg-pass.txt

for %%F in ("%INDIR%\*.pgp") do (
  echo Processing %%~nxF
  gpg --batch --yes --passphrase-file "%PASSFILE%" --output "%OUTDIR%\%%~nF"
--decrypt "%%F"
  if errorlevel 1 (
    echo FAILED: %%~nxF >> C:\FlowForce\PGP\logs\decrypt_errors.log
    move "%%F" "%FAILDIR%\"
  ) else (
    echo SUCCESS: %%~nxF >> C:\FlowForce\PGP\logs\decrypt_success.log
    move "%%F" "%PROCDIR%\"
  )
)
endlocal
```

8.2 Encryption Script (encrypt_all.bat)

```
@echo off
setlocal enabledelayedexpansion
SET INDIR=C:\FlowForce\PGP\outgoing\Plain
SET OUTDIR=C:\FlowForce\PGP\outgoing\Encrypted
SET PROCDIR=C:\FlowForce\PGP\outgoing\Processed
SET FAILDIR=C:\FlowForce\PGP\outgoing\Failed
SET RECIPIENT="partner@example.com"

for %%F in ("%INDIR%\*.*") do (
  echo Encrypting %%~nxF
  gpg --batch --yes --trust-model always --recipient %RECIPIENT% --output
"%OUTDIR%\%%~nxF.pgp" --encrypt "%%F"
  if errorlevel 1 (
    echo FAILED: %%~nxF >> C:\FlowForce\PGP\logs\encrypt_errors.log
    move "%%F" "%FAILDIR%\"
  ) else (
    echo SUCCESS: %%~nxF >> C:\FlowForce\PGP\logs\encrypt_success.log
    move "%%F" "%PROCDIR%\"
  )
```

```
)
endlocal
```

---

9. FlowForce Job Configuration

1. Open FlowForce Web UI.
2. Create job → **Execute Program**.
3. Program: `C:\Windows\System32\cmd.exe`
4. Arguments: `/c "C:\FlowForce\PGP\scripts\decrypt_all.bat"`
5. Working directory: `C:\FlowForce\PGP\scripts`
6. Run as: `FLOWFORCE_USER`
7. Schedule or trigger per requirements.
8. Configure email/SNMP alerts on job failure.
9. Repeat for `encrypt_all.bat`.

---

10. Task Scheduler Alternative

If FlowForce scheduling is not used, you can run encryption/decryption scripts with **Windows Task Scheduler**:

Steps to Configure:

1. Open **Task Scheduler** → `Create Task`.
2. **General Tab:**
   - Name: `PGP_Decryption_Task` (example).
   - Select `Run whether user is logged on or not`.
   - Use `FLOWFORCE_USER` or a dedicated service account.
3. **Triggers Tab:**
   - Click `New` → choose schedule (daily, hourly, every 5 min, etc.).
   - Optionally, set trigger on file arrival using external tools/scripts.
4. **Actions Tab:**
   - Action: `Start a program`.
   - Program/script: `C:\Windows\System32\cmd.exe`.
   - Arguments: `/c "C:\FlowForce\PGP\scripts\decrypt_all.bat"`.
   - Start in: `C:\FlowForce\PGP\scripts`.
5. **Conditions Tab:**
   - Uncheck `Start the task only if the computer is on AC power` (for servers).
6. **Settings Tab:**
   - Enable `Allow task to be run on demand`.

- Enable `Restart on failure` (set retries).

7. Save and enter credentials.

Repeat the same steps for an **encryption task** calling `encrypt_all.bat`.

---

11. Testing

- **Positive Test:** Encrypt a sample file with partner's key and ensure FlowForce decrypts it correctly.
- **Negative Test:** Corrupt a `.pgp` file and confirm FlowForce moves it to `Failed` folder.
- **End-to-End:** Exchange test files with partner until validation succeeds.

---

12. Error Handling & Alerts

- Log all failures in `C:\FlowForce\PGP\logs`.
- Send email alerts using FlowForce notifications or PowerShell `Send-MailMessage`.
- Escalate repeated failures to security and vendor teams.

---

13. Security Guidelines

- Restrict access to private keys and passphrase files.
- Rotate keys annually (or per policy).
- Maintain offline backup of private keys.
- Use separate keys for Dev/Test and Production.
- Generate and store a revocation certificate securely.

---

14. Vendor Onboarding Checklist

- Partner's public key and verified fingerprint.
- Filename conventions and encryption format.
- Test file exchange completed.
- Operational contacts established.

End of SOP