PGP Decrypt

Decrypts source files encrypted with PGP.

Name	Type	Required	Description
`Jitterbit.PGP.PrivateKeyData`	`string`	`false`	The ASCII representation of the private key. Alternatively, place the private key file directly on the Jitterbit Agent itself (assuming you have access to it), and set the data element `$Jitterbit.PGP.PrivateKeyFile` to the path of the file.
`Jitterbit.PGP.PrivateKeyFile`	`string`	`false`	The path to the private key file, in the case where the private key file is stored on the Jitterbit Agent. The file must be readable by the user that runs Jitterbit (more specifically the Jitterbit Process Engine). Alternatively, pass in the ASCII representation of the key itself in the data element `$Jitterbit.PGP.PrivateKeyData`.
`Jitterbit.PGP.Passphrase`	`string`	`true`	The passphrase with which the private key has been encrypted.
`Jitterbit.PGP.KeyDataForVerification`	`string`	`false`	If the message has been signed as well as encrypted, this data element should hold the ASCII representation of the key that will be used for verifying the message signature. This is typically the public key file of the message sender. The file must be placed on the Jitterbit Agent itself, and must be readable by the user that runs Jitterbit (more specifically the Jitterbit Process Engine). Alternatively, place the key file directly on the Jitterbit Agent (assuming you have access to it) and set the path to the file in the data element `$Jitterbit.PGP.KeyFileForVerification`. If neither of these data element are set the message signature will not be verified, even if the message is signed.
`Jitterbit.PGP.KeyFileForVerification`	`string`	`false`	If the message has been signed as well as encrypted, this data element should point to a key file containing the key that will be used for verifying the message signature. This is typically the public key file of the message sender. The file must be placed on the Jitterbit Agent itself, and must be readable by the user that runs Jitterbit (more specifically the Jitterbit Process Engine). Alternatively, pass in the ASCII representation of the key itself in the data element `$Jitterbit.PGP.KeyDataForVerification`. If neither of these data element are set the message signature will not be verified, even if the message is signed.
`Jitterbit.PGP.WriteLog`	`bool`	`false`	Turns plugin logging on or off. Logging is turned off by default; set this data element to true to turn on logging. The log messages are written to the file `jitterbit.plugin.pgp.decrypt.log` in the folder `[JITTERBIT_HOME]/log/plugin/`.

Plugin

PGP Decrypt 3.0 (.ZIP)

Related Articles

- Customizations > Plug-ins
- PGP Decrypt
- PGP Encrypt
- Plugins Available in Jitterbit Harmony
- Upgrading from Jitterbit v5.x to Harmony

Related Topics

- Apply Plug-ins (Design Studio)
- Plugin Library
- Plugins (Cloud Studio)

Last updated: Jan 31, 2020

Copyright © 1998 - 2019 Jitterbit, Inc.