3276828 - Updating pgp keys in pubring/secring of Cloud Integration tenant results in exception during decrypting/verifiyng a PGP message

Component: LOD-HCI-PI-CON-SOAP (OnDemand > SAP Cloud Integration > Process Integration > Connectivity > SOAP Adapter), Version: 2, Released On: 21.07.2023

Symptom

After pubring/secring have been updated following exception happens in Cloud Integration when the pgp keys are used:

com.sap.esb.camel.security.pgp.PgpException: An exception occurred during decrypting/verifiyng a PGP message. The PGP message may have been tampered. Reason: The input message body has an invalid format. The PGP decryption/verification processor expects a sequence of PGP packets of the form (entries in brackets are optional and ellipses indicate repetition, comma represents sequential composition, and vertical bar separates alternatives): Public Key Encrypted Session Key ..., Symmetrically Encrypted Data | Sym. Encrypted and Integrity Protected Data, Compressed Data, (One Pass Signature ...,) Literal Data, (Signature ...,), cause: **iaik.pgp.exceptions.PGPParsingException: Read invalid packet (ONE_PASS_SIGNATURE (TAG 4)) while decoding iaik.pgp.transferables.PGPMessage**

Environment

SAP Cloud Integration

Cause

The PGP keys are created incorrectly.

Resolution

Since SAP rolled out PGP cryptography it is recommended to use only **2.3.4 gpg4win** version for pgp key creation as the latest versions do not yet support PGP features or algorithms for pgp key creation. Make sure to use it on the following version: SAP Help - Installing gpg4win

See Also

SAP Help - Installing gpg4win

Keywords

pubring, secring, com.sap.esb.camel.security.pgp.PgpException:, An exception occurred during decrypting/verifiyng a PGP message., The PGP message may have been tampered., Reason: The input message body has an invalid format., The PGP decryption/verification processor expects a sequence of PGP packets of the form, (entries in brackets are optional and ellipses indicate repetition, comma represents sequential composition, and vertical bar separates alternatives):, Public Key Encrypted Session Key ..., Symmetrically Encrypted Data | Sym., Encrypted and Integrity Protected Data, Compressed Data, (One Pass Signature ...,) Literal Data, (Signature ...,), iaik.pgp.exceptions.PGPParsingException:, Read invalid packet, (ONE_PASS_SIGNATURE (TAG 4)), while decoding iaik.pgp.transferables.PGPMessage,

Attributes

Key	Value
Requires Action	0

Products

Products
Cloud Integration all versions