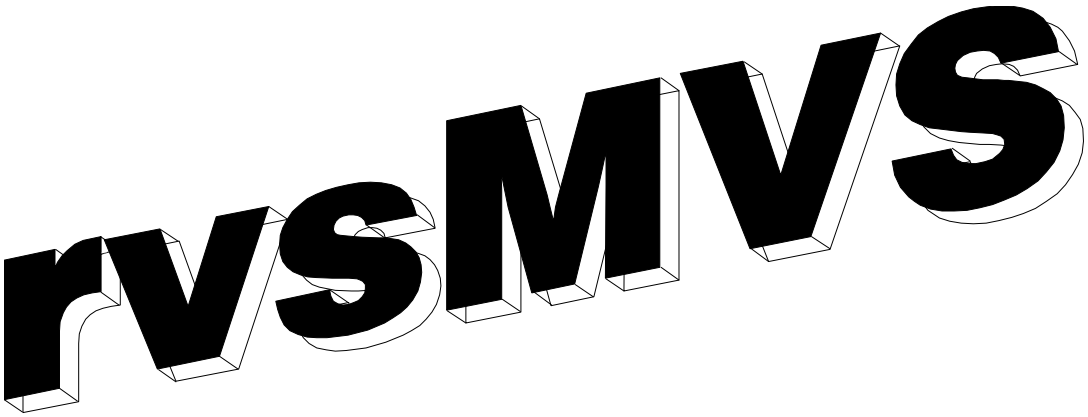
VOLKSWAGEN

T · · Systems · · ·



Release 04.02.02

Addendum
Online Encryption

2007/08/10

This documentation is valid for rvsMVS release 4

For rvsMVS the following documentations are provided:

rvsMVS Installation Manual (english)
Installation of rvs. Usefull for System Programmers

rvsMVS Benutzer Handbuch (german)
Manual for rvs Users

rvsMVS Operator Handbuch (german)
Manual for rvs Operator

rvsMVS Operation Manual (english)
Manual for rvs Operator

rvsMVS Messages and Codes (english)
Overview about rvs messages and abend codes

Distribution information will be given kindly:

T-Systems / gedas deutschland GmbH
Silke Peigert / Stephanie Begehold
BU rvs Systems
Pascalstr. 11
D-10587 Berlin

Tel. +49-30-3997-1367 / +49-30-3997-1537
Fax +49-30-3997-1994
Email mailto:Silke.Peigert@gedas.de
Email mailto:Stephanie.Begehold@gedas.de

Technical information will be given kindly:

T-Systems / gedas deutschland GmbH
BU rvs Systems
Pascalstr. 11
D-10587 Berlin

Tel. +49-30-3997-1777
Fax +49-30-3997-1994
Email mailto:rvs-service@gedas.de

Contents

1) Introduction

The feature ONLINE ENCRYPTION provides a 3DES encryption of each ODETTE data buffer during transmission.
Each ODETTE session, which sends datasets, creates a new 3DES encryption key. This key is transferred to the partner as RSA encrypted key.
The ONLINE ENCRYPTION uses the same key store like the rvsMVS feature OFFLINE ENCRYPTION (see installation manual for further information).

2) Steps To Configure ONLINE Encryption

The rvsMVS ONLINE ENCRYPTION uses the same RSA key store like OFFLINE ENCRYPTION. For further information refer the installation manual. If you already use OFFLINE ENCRYPTION with your partner station, you haven't to do the following steps.

- Create an own RSA key pair and import it to key store (see OFFLINE ENCRYPTION)
- Send your public key to the partner.
- Receive the public key of the partner and import it to your key store.

To enable ONLINE ENCRYPTION you have to set the parameter

SECURITY=ONL

in your STATIONS member for each station, which uses ONLINE ENCRYPTION.

NOTE: The feature ONLINE ENCRYPTION isn't negotiated. So both sides must configure the parameter for ONLINE ENCRYPTION. If one side doesn't configure ONLINE ENCRYPTION the transmitting of dataset will fail.
You can't use OFFLINE ENCRYPTION in conjunction with ONLINE ENCRYPTION.