Rocky Enterprise Linux 9.2 Manual Pages on command 'migrate-pubring-from-classic-gpg.1'

$ man migrate-pubring-from-classic-gpg.1

MIGRATE-PUBRING-FROM-CLASSIC-GPG(1)   General   Commands   Manual

MIGRATE-PUBRING-FROM-CLASSIC-GPG(1)

NAME

    migrate-pubring-from-classic-gpg - Migrate a public keyring from "classic" to "modern"

    GnuPG

SYNOPSIS

    migrate-pubring-from-classic-gpg [GPGHOMEDIR | --default]

DESCRIPTION

    migrate-pubring-from-classic-gpg migrates the public keyring in GnuPG home directory

    GPGHOMEDIR from the "classic" keyring format (pubring.gpg) to the "modern" keybox format

    using GnuPG versions 2.1 or 2.2 (pubring.kbx).

    Specifying --default selects the standard GnuPG home directory (looking at $GNUPGHOME

    first, and falling back to ~/.gnupg if unset.

OPTIONS

    -h, --help, --usage Output a short usage information.

DIAGNOSTICS

    The program sends quite a bit of text (perhaps too much) to stderr.

    During a migration, the tool backs up several pieces of data in a timestamped subdirectory

    of the GPGHOMEDIR.

LIMITATIONS

    The keybox format rejects a number of OpenPGP certificates that the "classic" keyring for?

    mat used to accept. These filters are defensive, since the certificates rejected are un?

    safe -- either cryptographically unsound, or dangerously non-performant. This means that

some migrations may produce warning messages about the migration being incomplete. This is generally a good thing!

Known limitations:

Flooded certificates

Some OpenPGP certificates have been flooded with bogus certifications as part of an attack on the SKS keyserver network (see https://tools.ietf.org/html/draft-dkg-openpgp-abuse-resistant-keystore-03#section-2.1).

The keybox format rejects import of any OpenPGP certificate larger than 5MiB.   As of GnuPG 2.2.17, if gpg encounters such a flooded certificate will retry the import while stripping all third-party certifications (see "self-sigs-only" in gpg(1)).

The typical error message when migrating a keyring with a flooded certificate will be something like:

error writing keyring 'pubring.kbx': Provided object is too large

OpenPGPv3 public keys (a.k.a. PGP-2 keys)

Modern OpenPGP implementations use so-called "OpenPGP v4" public keys. Older versions of the public key format have serious known problems.   See https://tools.ietf.org/html/rfc4880#section-5.5.2 for more details about and reasons for v3 key deprecation.

The keybox format skips v3 keys entirely during migration, and GnuPG will produce a message like:

skipped PGP-2 keys: 1

ENVIRONMENT VARIABLES

GNUPGHOME Selects the GnuPG home directory when set and --default is given.

GPG The name of the gpg executable (defaults to gpg).

SEE ALSO

gpg(1)

AUTHOR

Copyright (C) 2016 Daniel Kahn Gillmor for the Debian project. Please report bugs via the Debian BTS.