NAME

pcp2-protect-privatekey – Encryption of the private decryption exponent in a PCP RSA key

SYNOPSIS

pcp2-protect-privatekey encryptionkey | signingkey outfile

DESCRIPTION

pcp2-protect-privatekey is used to encrypt the RSA decryption exponent, the secret value stored in an RSA key file. Initially, after generation with **pcp2-generate-rsakeys** the decryption exponent is stored in the key file unprotected in clear text.

The program **pcp2-protect-privatekey** reads a user's passphrase and constructs a padding value using the passphrase and a file $HOME/.pcp/entropy, which protects the private decryption exponent in the outfile.

When the protected RSA key has replaced the unprotected one, the passphrase is neede to re-construct the padding value used to protect the private part, every time the decryption exponent is needed (to decrypt a file or to sign a file). For details see: https://senderek.ie/pcp2/pcp-2.0-security.php .

OPTIONS

none

NOTES

Full documentation: https://senderek.ie/pcp2

BUGS

Please report bugs to innovation@senderek.ie

AUTHORS

pcp2-protect-privatekey is written by Ralf Senderek <innovation@senderek.ie>.

COPYRIGHT

SEE ALSO

pcp2, pcp2-generate-rsakeys