NAME

pcp2 – The Pure Crypto Project Encryption System

SYNOPSIS

pcp2 -e|-d|-s|-ds|-v file

DESCRIPTION

pcp2 is a RSA key encryption software to protect email and other data files.

This manual is necessarily incomplete and assumes that you are already familiar with the basic concepts of public key cryptography and the Pure Crypto Project. You can find more information here: https://senderek.ie/pcp2

pcp2 can be used to perform the basic functions of encryption, decryption, signing and verifying of files. The discrete logarithm hash function SDLH (https://senderek.ie/sdlh) is used to hash data. The presence of a file in which the user's own hash key is stored is a precondition for the use of **pcp2**.

A user's hash key (hashmodulus and generator) can be generated with the program **sdlh-generate-hashkey**. The hashkey can be stored in a file ".hashkey" in the user's home directory or provided with the -key option.

OPTIONS

−e Encrypts a file with a trusted public encryption key in $HOME/.pcp/trusted-keys. The output file "file.pcp" contains only numbers giving no clue which key has been used to encrypt it.

−d Decrypts an encrypted file with the user's own private RSA encryption key "$HOME/.pcp/encryptionkey". In case a decryption error occurs, i.e the hash chain used for encryption can not be recovered completely, a chosen ciphertext attack is being assumed and nothing except a warning is written to the output file. The same result happens when a file containing only numbers cannot be decrypted because the cleartext has NOT been encrypted with the user's public encryption key.

−s Signs a file (clearsign) together with the signed data in one single file using the user's own private RSA signing key "$HOME/.pcp/signingkey". The input must be text data. To sign binary data the option "-ds" must be used (detached signature).

−ds Signs a file and stores the signature separately in a file with the .sig extension. This works for text and binary data.

−v Verifies a signed file (either clearsigned or signed separately) with the signer's public signingkey in $HOME/.pcp/trusted-keys.

NOTES

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

FILES

/usr/bin/systemd-ask-password
: This program is used to provide the passphrase based on a user's input to unlock a private RSA key.

/usr/share/pcp2/pure.py
: A library of functions used by pcp and other programs

$HOME/.pcp/trusted-keys
: The directory in which all public encryption or signing keys are stored. Every public key file must be signed with the user's own private RSA signing key to be regarded as trusted.

$HOME/.pcp/entropy
: This file is used to protect the private decryption exponent in a user's key file (encryptionkey or signingkey). It must contain at least 1 100 000 Bytes of truely random data.

BUGS

Please report bugs to innovation@senderek.ie

AUTHORS

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

COPYRIGHT

SEE ALSO

sdlh, pcp2-protect-privatekey, sdlh-generate-hashkey, pcp2-generate-rsakeys