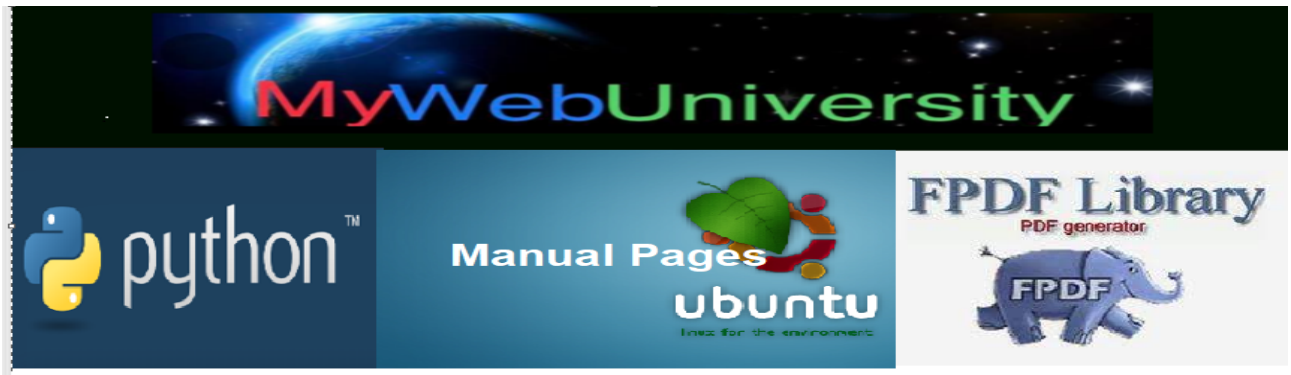

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'pdfsig.1'

$ man pdfsig.1

pdfsig(1) General Commands Manual pdfsig(1)

NAME

pdfsig - Portable Document Format (PDF) digital signatures tool

SYNOPSIS

pdfsig [options] [PDF-file] [Output-file]

DESCRIPTION

pdfsig verifies the digital signatures in a PDF document. It also displays the identity of each signer (commonName field and full distinguished name of the signer certificate), the time and date of the signature, the hash algorithm used for signing, the type of the signa? ture as stated in the PDF and the signed ranges with a statement wether the total document is signed. It can also sign PDF documents (options -add-signature or -sign).

pdfsig uses the trusted certificates stored either in the Network Security Services (NSS) Database or in GnuPG's S/MIME system (gpgsm).

pdfsig also uses the Online Certificate Status Protocol (OCSP) (refer to http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol) to look up the certificate online and check if it has been revoked (unless -no-ocsp has been specified).

If the NSS backend is used, the NSS Database is searched for in the following locations:

1 If the -nssdir option is specified, the directory specified by this option.

2 The NSS Certificate database in the default Firefox profile. i.e. $HOME/.mozilla/firefox/*.default*.

3 System?s NSS Certificate database in /etc/pki/nssdb.

4 User?s NSS Certificate database in $HOME/.pki/nssdb.

If the GPG backend is used, the S/MIME certificate is read from $GNUPGHOME, defaulting to

$HOME/.gnupg

OPTIONS

-nssdir [prefix]directory

Specify the database directory containing the certificate and key database files. See certutil(1) -d option for details of the prefix. If not specified the other search locations described in DESCRIPTION are used.

-nss-pwd password

Specify the password needed to access the NSS database (if any).

-nocert

Do not validate the certificate.

-no-ocsp

Do not perform online OCSP certificate revocation check (local Certificate Revocation Lists (CRL) are still used).

-assert-signer fpr_or_file

This option checks whether the signature covering the full document been made with the specified key. The key is either specified as a fingerprint or a file listing fingerprints. The fingerprint must be given or listed in compact format (no colons or spaces in between). If fpr_or_file specifies a file, empty lines are ignored as well as all lines starting with a hash sign. Only available for GnuPG backend

-no-appearance

Do not add appearance information when signing existing fields (signer name and date).

-aia Enable the use of Authority Information Access (AIA) extension to fetch missing cer? tificates to build the certificate chain.

-dump Dump all signatures into current directory in their native format. Most likely it is either a unpadded or zero-padded CMS/PKCS7 bundle.

-add-signature

Add a new signature to the document.

-new-signature-field-name name

Specifies the field name to be used when adding a new signature. A random ID will be used by default.

-sign field

Sign the document in the specified signature field present in the document (must be

unsigned). Field can be specified by field name (string) or the n-th signature field in the document (integer).

-nick nickname

Use the certificate with the given nickname for signing (NSS backend). If nickname starts with pkcs11:, it's treated as PKCS#11 URI (NSS backend). If the nickname is given as a fingerprint, it will be the certificate used (GPG backend)

-backend backend

Use the specified backeng for cryptographic signatures

-kpw password

Use the given password for the signing key (this might be missing if the key isn't password protected).

-digest algorithm

Use the given digest algorithm for signing (default: SHA256).

-reason reason

Set the given reason string for the signature (default: no reason set).

-enable-pgp

Enable pgp signatures in the GnuPG backend. Only available for GnuPG backend.

-etsi Create a signature of type ETSI.CAdES.detached instead of adbe.pkcs7.detached.

-list-nicks

List available nicknames in the NSS database.

-list-backends

List available backends for cryptographic signatures

-v Print copyright and version information.

-h Print usage information. (-help and --help are equivalent.)

EXAMPLES

pdfsig signed_file.pdf

Displays signature info for signed_file.pdf.

pdfsig input.pdf output.pdf -add-signature -nss-pwd password -nick my-cert -reason 'for fun!'

Creates a new pdf named output.pdf with the contents of input.pdf signed by the 'my-cert' certificate.

pdfsig input.pdf output.pdf -add-signature -nss-pwd password -nick 'pkcs11:token=smart?card0;object=Second%20certificate;type=cert'

Same, but uses a PKCS#11 URI as defined in IETF RFC 7512 to select the certificate to be used for signing.

pdfsig input.pdf output.pdf -sign 0 -nss-pwd password -nick my-cert -reason 'for fun!'

Creates a new pdf named output.pdf with the contents of input.pdf signed by the 'my-cert' certificate. input.pdf must have an already existing un-signed signature field.

AUTHOR

SEE ALSO

pdfdetach(1), pdffonts(1), pdfimages(1), pdfinfo(1), pdftocairo(1), pdftohtml(1), pdftoppm(1), pdftops(1), pdftotext(1) pdfseparate(1), pdfunite(1) certutil(1)