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 signature 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 in the Network Security Services (NSS) Database.

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http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol) to look up the certificate online and check if it has been revoked (unless -no-ocsp has been specified).

The NSS Database is searched for in the following locations:

- If the −nssdir option is specified, the directory specified by this option.
- The NSS Certificate database in the default Firefox profile. i.e. $HOME/.mozilla/firefox/*.default.
- The NSS Certificate database in /etc/pki/nssdb.

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).

−aia Enable the use of Authority Information Access (AIA) extension to fetch missing certificates to build the certificate chain.

−dump Dump all signatures into current directory.

−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 n
Sign the document in the n-th signature field present in the document (must be unsigned).

−nick nickname
Use the certificate with the given nickname for signing.

−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).

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

−list-nicks
List available nicknames in the NSS database.

−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 -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)