NAME

ksi pubfile - Verify and dump KSI publications file with KSI command-line tool.

SYNOPSIS

ksi pubfile -P *URL* **--dump**

ksi pubfile -P *URL* **-v --cnstr** *oid=value* ... [**-V** *cert.pem*]... [**-W** *dir*]... [*more_options*]

ksi pubfile -P *URL* **-o** *pubfile.bin* **--cnstr** *oid=value* ... [**-V** *cert.pem*]... [**-W** *dir*]... [*more_options*]

ksi pubfile -T *time* **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] [*more_options*]

DESCRIPTION

Verifies and dumps the content of KSI publications file. The KSI publications file contains information on all the existing publications records and the PKI certificates that are used to verify the calendar authentication records of KSI signatures.

OPTIONS

-P *URL* Specify publications file URL (or file with URI scheme 'file://').

--cnstr *oid=value*

Specify the OID of the PKI certificate field (e.g. e-mail address) and the expected value to qualify the certificate for verification of publications file's PKI signature. At least one constraint must be defined. All values from lower priority source are ignored (see **ksi-conf**(5) for more information).

For more common OIDs there are convenience names defined:

- **E** or **email** for OID 1.2.840.113549.1.9.1
- **CN** or **cname** for OID 2.5.4.3
- **C or country** for OID 2.5.4.6
- **O** or **org** for OID 2.5.4.10

-v Perform publications file verification. Note that when **-o** is used to save publications file, the verification is performed implicitly.

-V *file* Specify the certificate file in PEM format for publications file verification. All values from lower priority source are ignored (see **ksi-conf**(5)).

-W *dir* Specify the OpenSSL-style trust store directory for publications file's PKI signature verification. All values from lower priority source are ignored (see **ksi-conf**(5)).

-o *file* Specify the output file path to store publications file. Use '**-**' as file name to redirect publications file binary stream to *stdout*. Publications file is always verified before saving.

-X *URL*

Specify the extending service (KSI Extender) URL. Supported URL schemes are: *http*, *https*, *ksi+http*, *ksi+https* and *ksi+tcp*. It is possible to embed HTTP or KSI user info into the URL. With *ksi+* suffix (e.g. ksi+http//user:key@...), user info is interpreted as KSI user info, otherwise (e.g. http//user:key@...) the user info is interpreted as HTTP user info. User info specified with **--ext-user** and **--ext-key** will overwrite the embedded values.

--ext-user *str*

Specify the username for extending service.

--ext-key *str*

Specify the HMAC key for extending service.

--ext-hmac-alg *alg*

Hash algorithm to be used for computing HMAC on outgoing messages towards KSI extender. If not set, default algorithm is used. Use **ksi -h** to get the list of supported hash algorithms.

-T *time* Specify the time to create a publication string for as the number of seconds since 1970-01-01 00:00:00 UTC or time string formatted as "YYYY-MM-DD hh:mm:ss".

-d Print detailed information about processes and errors to *stderr*.

--dump
Dump publications file in human-readable format to *stdout*. Without any extra flags publications file verification is not performed.

--conf *file*
Read configuration options from given file. It must be noted that configuration options given explicitly on command line will override the ones in the configuration file (see **ksi-conf**(5) for more information).

--log *file*
Write **libksi** log to given file. Use '-' as file name to redirect log to *stdout*.

EXIT STATUS

See **ksi**(1) for more information.

EXAMPLES

In the following examples it is assumed that KSI service configuration options (URLs, access credentials) are defined. See **ksi-conf**(5) for more information.

1 To dump the publications file from default URL:

ksi pubfile --dump

2 To dump the publications file *pubfile.bin* on local file system (verification is not performed):

ksi pubfile --dump -P *file://pubfile.bin*

3 To verify a publications file *pubfile.bin* from local disk:

ksi pubfile -v -P *file:///home/user/publications/pubfile.bin*

4 To download, verify and save the publications file to *pubfile.bin* from default URL (verification is performed automatically when saving):

ksi pubfile -o *pubfile.bin* **--cnstr** *email=publications@guardtime.com*

5 To verify the publications file with only certificates defined on command line:

ksi pubfile -v -V *certificate_1.bin* **-V** *certificate_2.bin* **--cnstr** *email=publications@guardtime.com*

6 To create a publication string:

ksi pubfile -T "*2015-10-15 00:00:00*"

ENVIRONMENT

Use the environment variable **KSI_CONF** to define the default configuration file. See **ksi-conf**(5) for more information.

AUTHOR

Guardtime AS, http://www.guardtime.com/

SEE ALSO

ksi(1), **ksi-sign**(1), **ksi-verify**(1), **ksi-extend**(1), **ksi-conf**(5)