NAME

ksi extend - Extend KSI signature with KSI command-line tool.

SYNOPSIS

ksi extend -i *in.ksig* [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... [*more_options*]

ksi extend -i *in.ksig* [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... **--pub-str** *str* [*more_options*]

ksi extend -i *in.ksig* [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-T** *time* [*more_options*]

DESCRIPTION

Extends the given KSI signature to the time of given publication. After signature is extended and the corresponding publication record is attached, the signature can be verified by publication-based verification where only trusted publications file or a publication string in printed media is needed to perform the verification. See **ksi-verify**(1) for details.

User must have access to KSI extending service and trusted KSI publications file to extend the KSI signature. By default signature is extended to the earliest available publication. Use the option **--pub-str** to extend signature to the publication denoted by the given publication string. It is also possible to extend to the specified time with option **-T** but this is not recommended as the extended signature will have no calendar authentication nor publication record and can only be verified by calendar-based verification.

OPTIONS

-i *in.ksig*

Specify the file path to the KSI signature file to be extended. Use '-' as the path to read the signature from *stdin*.

-o *out.ksig*

Specify the output file path for the extended signature. Use '-' as the path to redirect the signature binary stream to *stdout*. If not specified, the signature is saved to <in.ksig>.ext.ksig (or <in.ksig>ext_<nr>.ksig where *nr* is auto-incremented counter if the output file already exists). If specified, existing file is always overwritten.

-X *URL*

Specify the extending service (KSI Extender) URL.

--ext-user *user*

Specify the username for extending service.

--ext-key *key*

Specify the HMAC key for extending service.

-P *URL* Specify the 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 common OID's 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

--pub-str *str*

Specify the publication record as publication string to extend signature to.

-T *time* Define the publication time to extend to as the number of seconds since 1970-01-01 00:00:00 UTC or time formatted as "YYYY-MM-DD hh:mm:ss".

-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 an OpenSSL-style trust store directory for publications file verification. All values from lower priority source are ignored (see **ksi-conf**(5)).

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

--dump
Dump extended signature and verification info in human-readable format to *stdout*.

--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 extend a signature *sig.ksig* to the earliest available publication and save it as *ext.ksig*:

ksi extend -i *sig.ksig* **-o** *ext.ksig*

2 To extend a signature *sig.ksig* to s specified publication (the publication string available from Financial Times, ISSN: 0307-1766, 2016-03-17 given as example):

ksi extend -i *sig.ksig* **-o** *ext.ksig* **--pub-str** *AAAAAA-CW45II-AAKWRK-F7FBNM-KB6FNV-DYYFW7-PJQN6F-JKZWBQ-3OQYZO-HCB7RA-YNYAGA-ODRL2V*

3 To extend a signature *sig.ksig* to specified calendar time *2015-05-05 00:00:00* and save it as *ext.ksig*:

ksi extend -i *sig.ksig* **-o** *ext.ksig* **-T** *"2015-05-05 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-pubfile**(1), **ksi-conf**(5)