NAME

logksi extend - Extend KSI signatures in log signature file.

SYNOPSIS

logksi extend [*logfile*] [**-o** *out.logsig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... [*more_options*]

logksi extend [*logfile*] [**-o** *out.logsig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... **--pub-str** *str* [*more_options*]

logksi extend [*logfile*] [**-o** *out.logsig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-T** *time* [*more_options*]

logksi extend [*logfile*] [**-o** *out.logsig*] **--conf** *logksi.conf* [*more_options*]

DESCRIPTION

Extends the KSI signatures in a log signature file of the given *logfile* to the time of given publication. KSI signatures are expected to be found from *logfile.logsig*. If no *logfile* is specified, the input is expected from *stdin*.

After the signatures are extended and the corresponding publication records are attached, the signatures 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 **logksi-verify**(1) for details.

User must have access to KSI extending service and trusted KSI publications file to extend the log signatures. By default the signatures are extended to the earliest available publication. Use the option **--pub-str** to extend signatures 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 signatures will have no calendar authentication nor publication record and can only be verified by calendar-based verification policy.

Note that all KSI signatures present in the log signature file will be attempted to extend to the same publication. If for some reason the extending of at least one signature fails, none of the signatures are extended.

If both, input and output values are left unspecified, the *stdin* and *stdout* are used, respectively.

OPTIONS

-o *out.logsig*
: Specify the output file path for the extended log signature file. Default output file is *logfile.logsig*, and in this case the backup of the original *logfile.logsig* will be saved in *logfile.logsig.bak*. If extending fails, the newly created *logfile.logsig* will be deleted and the original *logfile.logsig* will be restored from the backup file. If a file with the name specified already exists, it will be overwritten and backup file will not be created. Use '-' as file name to redirect the output as binary stream to *stdout*.

-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 **logksi-conf**(5)).

  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

--pub-str *str*
Specify the publication record as publication string to extend the signatures to.

-T *time* Specify 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 **logksi-conf**(5)).

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

--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 **logksi-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 **logksi**(1) for more information.

EXAMPLES

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

1 To extend the signatures in */var/log/secure.logsig* to the earliest available publication and save the file as */var/log/secureExt.logsig*:

logksi extend */var/log/secure* **-o** */var/log/secureExt.logsig*

2 To extend the signatures in */var/log/secure.logsig* to s specified publication (the publication string available from Financial Times, ISSN: 0307-1766, 2016-03-17 given as example) and save the result with default name */var/log/secure.logsig*:

logksi extend */var/log/secure* **--pub-str** *AAAAAA-CW45II-AAKWRK-F7FBNM-KB6FNV-DYYFW7-PJQN6F-JKZWBQ-3OQYZO-HCB7RA-YNYAGA-ODRL2V*

3 To extend the signatures in */var/log/secure.logsig* to specified calendar time *2015-05-05 00:00:00* and save the file as */var/log/secureExt.logsig*:

logksi extend */var/log/secure* **-o** */var/log/secureExt.logsig* **-T** *"2015-05-05 00:00:00"*

ENVIRONMENT

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

AUTHOR

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

SEE ALSO

logksi(1), **logksi-sign**(1), **logksi-integrate**(1), **logksi-verify**(1), **logksi-conf**(5)