

NAME

logksi sign - Sign unsigned blocks for the given log file.

SYNOPSIS

logksi sign *<logfile>* [-o *<out>.logsig*] -S *URL* [--aggr-user *user* --aggr-key *key*] [*more options*]

logksi sign --sig-from-stdin [-o *<out>.logsig*] -S *URL* [--aggr-user *user* --aggr-key *key*] [*more options*]

DESCRIPTION

Signs the unsigned log blocks in a log signature file of a given *<logfile>*. The name of the log signature file located in the same directory as the *<logfile>* is expected to be *<logfile>.logsig* or *<logfile>.gtsig*. Alternatively, if no *<logfile>* is specified, the **--sig-from-stdin** option should be used to read the log signature file from the *stdin*. If neither the *<logfile>* nor **--sig-from-stdin** option is given, help text is returned.

logksi sign provides the recovery signing functionality for cases when some log blocks have been left unsigned during routine signing/logging. For instance, when the KSI service was not reachable.

User must have access to KSI signing service (KSI Aggregator) for signing.

OPTIONS

<logfile>

Name of the log file whose unsigned log blocks should be signed. If *<logfile>* is specified, the **--sig-from-stdin** option cannot be used.

--sig-from-stdin

Use to read the log signature file from *stdin*. If no output file is specified with **-o**, the result will be returned to *stdout*.

-o *<out>.logsig*

Specify the name of the output log signature file. If not specified, the input file *<logfile>.logsig* is modified. The backup of the original log signature file will be saved to *<logfile>.logsig.bak*. If the output file name is explicitly specified, an existing file will always be overwritten and no backup file will be created. Use '-' as file name to redirect the output as a binary stream to *stdout*.

-S *URL* Specify the signing service (KSI Aggregator) URL.

--aggr-user *user*

Specify the username for signing service.

--aggr-key *key*

Specify the HMAC key for signing service.

--aggr-hmac-alg *alg*

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

--aggr-pdu-v *str*

Specify the KSIAP (KSI Aggregation Protocol) PDU version. Valid values are *v1* and *v2*. Note that use of *v1* is **deprecated** and use of *v2* is recommended.

--insert-missing-hashes

Repair the log signature by inserting missing final tree hashes. Final tree hashes might be missing if the Merkle tree is not perfectly balanced. If the option is not used, a warning message is printed about missing hashes with a recommendation to run **logksi sign** again with the **--insert-missing-hashes** option. Inserting missing hashes improves verifiability, but a log signature without final tree hashes is verifiable as well.

-d

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

--show-progress

Print signing progress. Only valid with **-d**.

--conf *file*

Read configuration options from the 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 the given file. Use '-' as file name to redirect the 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 sign unsigned blocks in log signature file */var/log/secure.logsig* and save the amended log signature file in */var/log/secure-signed.logsig*:

logksi sign /var/log/secure -o /var/log/secure-signed.logsig

- 2 To sign unsigned blocks in log signature file */var/log/secure.logsig* and save the result in the same file after creating the respective backup file */var/log/secure.logsig.bak*:

logksi sign /var/log/secure

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-extend(1)**, **logksi-extract(1)**, **logksi-integrate(1)**, **logksi-verify(1)**, **logksi-conf(5)**