NAME

ksi sign - Guardtime command-line tool for creating KSI Signatures.

SYNOPSIS

ksi sign -i *input* [**-o** *out.ksig*] **-S** *URL* [**--aggr-user** *user* **--aggr-key** *key*] [**-H** *alg*] [**--data-out** *file*] [**--dump**] [*more options*]

DESCRIPTION

This is a general signing tool for Guardtime Keyless Signature services. As the signature created contains a calendar authentication record as trust anchor it can be verified by key-based and calendar-based verification only (see **ksi-verify**(1)). **The signature should be extended as soon as the first publication becomes available**. After the signature is extended (see **ksi-extend**(1)) it is linked with a publication and can be verified by publication-based verification that relies only on the hash functions.

OPTIONS

-i *data* Files path to file to be hashed or data hash imprint to extract the hash value that is going to be signed. Use '-' as file name to read data to be hashed from *stdin*. Hash imprint format: <*alg*>:<*hash in hex*>. Call **ksi -h** to get the list of supported hash algorithms.

-o *file* Output file name to store signature token. Use '-' as file name to redirect signature binary stream to *stdout*. If not specified signature is saved to the path described as <input files path>(nr).ksig, where *(nr)* is generated serial number if file name already exists. If specified will always overwrite the existing file.

-H *alg* Use a specific hash algorithm to hash the file to be signed. Call **ksi -h** to get the list of supported hash algorithms.

-S *URL* Specify signing service URL.

--aggr-user *str*
User name for signing service.

--aggr-key *str*
HMAC Key for signing service.

--data-out *file*
Save signed data to file. Use when signing a stream. Use '-' as file name to redirect data being hashed to *stdout*.

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

--dump
Dump signature created to *stdout*.

--conf *file*
Specify a configurations file to override default service information. It must be noted that service info from command-line will override the configurations file. See **ksi**(1) and **ksi-conf**(5) for more information.

--log *file*
Write libksi log into 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 default service URLs are defined (see **ksi**(1) for more information).

1 To sign a file *file* and save signature to *sig.ksig* call:
ksi sign -i *file* **-o** *sig.ksig*

2 To sign a data hash (hashed with SHA256) and save the resulting signature to file *sig.ksig* call:

ksi sign -i *SHA-256:c8ef6d57ac28d1b4e95a513959f5fcdd0688380a43d601a5ace1d2e96884690a* -o *sig.ksig*

3 To sign a data file *file* with non-default algorithm *SHA1* call:
ksi sign -i *file* **-H** *SHA1* **-o** *sig.ksig*

4 To sign a stream (stdin), save data from stream to *file* and save signature to *sig.ksig* call:
ksi -s -i - --data-out *file* **-o** *sig.ksig*

ENVIRONMENT

Environment variable **KSI_CONF** can be defined to set default KSI configurations file. See **ksi**(1) and **ksi-conf**(5) for more information.

AUTHOR

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

SEE ALSO

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