NAME

ksi.conf - Keyless Signature Infrastructure (KSI) command-line tool configuration file.

DESCRIPTION

The KSI command-line tool has several configuration options, most of them are related to the KSI service configuration (e.g. KSI signing service URL and access credentials). The configuration options are described in the **OPTIONS** section below. Ways to define the options are:

- directly on command line (highest priority)
- in a file specified by the **--conf** command-line argument
- in a file specified by the **KSI_CONF** (lowest priority)

If a configuration option is specified in more than one source, the source with the highest priority will be used (i.e. command-line argument will override file specified by **--conf** or **KSI_CONF**).

While defining options, a short parameter or multiple flags must have prefix '**-**' and long parameters have prefix '**--**'. If some parameter values contain whitespace characters, double quote marks (**"**) must be used to wrap the entire value. If double quote mark or backslash have to be used inside the value part, an escape character (\) must be typed before the charcater(**"** or \\). If configuration option with unknown or invalid key-value pairs is used, an error is generated.

In configuration file each key-value pair must be placed on a single line. For commenting, start the line with **#**.
In case of **-V**, **-W** and **-P** options file location is interpreted as relative to the configuration file, if full path is not defined.
See **EXAMPLES** for more information.

OPTIONS

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

--aggr-user *str*
Specify the username for signing service.

--aggr-key *str*
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 **ksi -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 *v1* is **legacy** implementation and will be fully replaced with *v2* in the future.

-H *alg* Use the given hash algorithm to hash the file to be signed. If not set, the default algorithm is used. Use **ksi -h** to get the list of supported hash algorithms. If used in combination with **--apply-remote-conf**, the algorithm parameter provided by the server will be ignored.

-X *URL*
Specify the extending service (KSI Extender) URL.

--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.

--ext-pdu-v *str*
Specify the KSIEP (KSI Extension Protocol) PDU version. Valid values are *v1* and *v2*. Note that *v1* is **legacy** implementation and will be fully replaced with *v2* in the future.

--max-lvl *int*
Set the maximum depth (0 - 255) of the local aggregation tree (default: 0). It must be noted that when using masking (**--mask**) or embedding of the metadata (**--mdata**), the maximum count of document hash values that could be signed during a single local aggregation round will be reduced. To enable signing in multiple local aggregation rounds see **--max-aggr-rounds**. If used in combination with **--apply-remote-conf**, where service *maximum level* is provided, the smaller value is applied.

--max-aggr-rounds *int*
Set the upper limit of local aggregation rounds that may be performed (default: 1).

--mdata-cli-id *str*
Specify the client ID as a string which will be embedded into the signature as metadata. It is mandatory part of the metadata.

--mdata-mac-id *str*
Specify the machine ID as a string which will be embedded into the signature as metadata. It is optional part of the metadata.

--mdata-sqn-nr [*int*]
Specify the incremental (sequence number is incremented in every aggregation round) sequence number of the request as integer which will be embedded into the signature as metadata. If the parameter is given without the argument, 0 is used. It is optional part of metadata.

--mdata-req-tm
Embed the request time extracted from the machine clock into the signature as metadata. It is optional part of metadata.

-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.

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 *file* Specify the certificate file in PEM format for publications file verification.

-W *dir* Specify an OpenSSL-style trust store directory for publications file verification.

-C *int* Specify allowed connect timeout in seconds. This is not supported with TCP client.

-c *int* Specify allowed network transfer timeout, after successful connect, in seconds.

--publications-file-no-verify
Force the KSI tool to trust the publications file without verifying it. This option can only be defined on command line to avoid the usage of insecure configuration files. Note that the **option is insecure** and may only be used for testing.

--apply-remote-conf
Obtain and apply additional configuration data from service server. See **ksi-sign**(1) and **ksi-extend**(1) for more information.

--inst-id [*int*]
An integer (>= 0) to identify the sender instance that is constant during the KSI tool process lifetime. It should stay constant or increase every time KSI tool is executed as server may drop future messages with lower *instance identifier* values. When specified as integer, the constant value is used. When specified without argument, unix time is used in place of a constant. If not specified, *instance identifier* is not included to the request header. Note that this value only affects KSI protocol PDUs.

--msg-id [*int*]
An integer (>= 1) to identify the requests within KSI tool process lifetime. The *message identifier* value is increased after every request. When specified without argument, 1 is used. If not specified *message identifier* is not included to the request header. Note that this value only affects KSI protocol PDUs.

ENVIRONMENT

Program **ksi**(1) uses environment variable **KSI_CONF** to point to the default configuration file.

EXAMPLES

An example of configuration file:

```
# --- BEGINNING ---
#
# KSI Signing service parameters:
-S http://example.gateway.com:3333/gt-signingservice
--aggr-user anon
--aggr-key anon

# Override default hash algorithm:
-H SHA2-512

# KSI Extending service parameters:
# Note that ext-key real value is &h/J"kv\G##
-X http://example.gateway.com:8010/gt-extendingservice
--ext-user anon
--ext-key "&h/J\"kv\\G##"

# KSI Publications file:
-P http://verify.guardtime.com/ksi-publications.bin
--cnstr email=publications@guardtime.com
--cnstr "org=Guardtime AS"
#
# --- END ---
```

AUTHOR

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

SEE ALSO

ksi-sign(1), **ksi-verify**(1), **ksi-extend**(1), **ksi-pubfile**(1)