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 configurations 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 configurations 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.

-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.

--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**.

--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 PKI signature. At least one constraint must be defined.

>   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

-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*   Define allowed connect timeout in seconds. This is not supported with TCP client.

-c *int*   Define 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. It must be noted that the **option is insecure** and may only be used for testing.

ENVIRONMENT

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

EXAMPLES

>   An example of configurations file:

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