NAME

logksi.conf - Log signature command-line tool configuration file.

DESCRIPTION

The log signature tool has has several configuration options, most of them 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; or
- 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 a 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 a double quote mark or backslash has to be used inside the value part, an escape character (\) must be typed before the charcater. If a configuration option with unknown or invalid key-value pairs is used, an error is generated.

In the 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 *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 *v1* is **deprecated** implementation and will be fully replaced with *v2* in the future.

-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.

--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 **logksi -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 use of *v1* is **deprecated** and use of *v2* is recommended.

-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 log signature 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 **logksi**(1) uses environment variable **KSI_CONF** to point to the default configuration file.

EXAMPLES

An example of a configuration 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

logksi(1), **logksi-extend**(1), **logksi-extract**(1), **logksi-integrate**(1), **logksi-sign**(1), **logksi-verify**(1),