

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. There are following ways to specify these configuration options:

- 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 (e.g. both directly on command-line argument and in a configuration file) the source with the highest priority will be used. 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 character (\" 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. Start the line with **#** to write a comment. Not full paths (V, W and P with URI scheme file://) are interpreted as relative to the configurations file.

OPTIONS

-S URL Signing service (KSI Aggregator) URL.

--aggr-user str
Username for signing service.

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

-X URL
Extending service (KSI Extender) URL.

--ext-user str
Username for extending service.

--ext-key str
HMAC key for extending service.

-P URL Publications file URL (or file with URI scheme 'file://').

--cnstr oid=value
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 Certificate file in PEM format for publications file verification.

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

-C int Network connect timeout in seconds (is not supported with TCP client).

-c int Network transfer timeout, after successful connect, in seconds.

--publications-file-no-verify

A flag to force the tool to trust the publications file without verifying it. The flag can only be defined on command-line to avoid the usage of insecure configurations 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:
# Note that ext-key real value is &h/J"kv\G##
-X http://example.gateway.com:8010/gt-extending-service
--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)