

**NAME**

**ksi.conf** - KSI (Keyless Signature Infrastructure) service configuration file.

**DESCRIPTION**

This file is read by ksi command-line tool **ksi(1)** as KSI service configurations file. Configurations file is composed with the following parameters described under section **OPTIONS**. If configurations file with unknown or invalid key-value pairs is used, an error is generated until user applies all the fixes needed. All **ksi(1)** components that use KSI services must accept the configurations file (option **--conf file**). It must also be possible to define exactly the same parameters on command-line to override values from configurations file.

All the key-value pairs must be placed one per line. A short parameter or multiple flags must have prefix **-** and long parameters must have prefix **--**. To write a comment start the line with **#**. If some parameter values contain whitespace characters a double quote marks **"** must be used to wrap the entire value. If double quote mark **"** have to be used inside the value part an escape character **\** must be typed before the quote mark like that **\"**.

**OPTIONS**

- S url** Specify signing service URL.
- aggr-user str**  
User name for signing service.
- aggr-key str**  
HMAC Key for signing service.
- X url** Specify extending service URL.
- ext-user str**  
User name for extending service
- ext-key str**  
HMAC Key for extending service.
- P url** Specify publications file URL (or file with uri scheme 'file://').
- cnstr oid=value**  
OID and its expected value to verify publications file PKI signature. At least one constraint must be defined to be able to verify publications file but it is possible to define more.
- V file** Specify an OpenSSL-style trust store file for publications file verification.
- W dir** Specify an OpenSSL-style trust store directory for publications file verification.
- c int** Set network transfer timeout, after successful connect, in s.
- C int** Set network Connect timeout in s (is not supported with tcp client).
- 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://ksigw.test.guardtime.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://ksigw.test.guardtime.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), **ksi-conf**(5)