NAME

ksi extend - Extend KSI signature with KSI command-line tool.

SYNOPSIS

ksi extend [**-i** *in.ksig*] [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... [*more_options*] [**--**] *input*...

ksi extend [**-i** *in.ksig*] [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... **--pub-str** *str* [*more_options*] [**--**] *input*...

ksi extend [**-i** *in.ksig*] [**-o** *out.ksig*] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-T** *time* [*more_options*] [**--**] *input*...

ksi extend -X *URL* [**--ext-user** *user* **--ext-key** *key*] **--dump-conf**

DESCRIPTION

Extends the given KSI signature to the time of given publication. After signature is extended and the corresponding publication record is attached, the signature can be verified by publication-based verification where only trusted publications file or a publication string in printed media is needed to perform the verification. See **ksi-verify**(1) for details.

User must have access to KSI extending service and trusted KSI publications file to extend the KSI signature. By default signature is extended to the earliest available publication. Use the option **--pub-str** to extend signature to the publication denoted by the given publication string. It is also possible to extend to the specified time with option **-T** but this is not recommended as the extended signature will have no calendar authentication nor publication record and can only be verified by calendar-based verification.

OPTIONS

-i *in.ksig*

Specify the file path to the KSI signature file to be extended. Use '**-**' as the path to read the signature from *stdin*. Flag **-i** can be omitted when specifying the input. Without **-i** it is not possible to sign files that look like command line parameters (e.g. -a, --option). To interpret all inputs as regular files no matter what the file's name is, see parameter **--**.

-o *out.ksig*

Specify the output file path for the extended signature. Use '**-**' as the path to redirect the signature binary stream to *stdout*. If not specified, the output is saved to the same directory where the input file is located. If specified as directory, all the signatures are saved there. When signature's output file name is not explicitly specified the signature is saved to *<input[.E]>.ext.ksig* or *<input[.E]>.ext_<nr>.ksig* where *E* is input file extension that is NOT equal to *ksig* and *nr* is auto-incremented counter if the output file already exists. If output file name is explicitly specified, will always overwrite the existing file.

-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 **ksi -h** to get the list of supported hash algorithms.

-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. All values from lower priority source are ignored (see **ksi-conf**(5)).

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

--pub-str *str*
Specify the publication record as publication string to extend signature to.

--replace-existing
Replace input KSI signature file with successfully extended version. During the saving process old signature is renamed and is handled as temporary buffer for the original file. If saving of extended signature is successfully performed the old signature is deleted. In cases of failures the old signatures may be left renamed as <*original input file*>.*backup*.<*20 random decimal digits*> and is not deleted.

-T *time* Specify the publication time to extend to as the number of seconds since 1970-01-01 00:00:00 UTC or time formatted as "YYYY-MM-DD hh:mm:ss". Note that if the time is chosen to be equal to an existing publication record's time, the publication record is not added to the signature; use **--pub-str** for publication records.

-V *file* Specify the certificate file in PEM format for publications file verification. All values from lower priority source are ignored (see **ksi-conf**(5)).

-W *dir* Specify an OpenSSL-style trust store directory for publications file verification. All values from lower priority source are ignored (see **ksi-conf**(5)).

-- If used, **everything** specified after the token is interpreted as **KSI signature input file** (command-line parameters (e.g. --conf, -d) and *stdin* (-) are all interpreted as regular files).

-d Print detailed information about processes and errors to *stderr*.

--dump
Dump extended signature and verification info in human-readable format to *stdout*.

--dump-conf
Dump extender (URL specified by **-X** parameter) configuration in human-readable format to *stdout*.

--conf *file*
Read configuration options from given file. It must be noted that configuration options given explicitly on command line will override the ones in the configuration file. See **ksi-conf**(5) for more information.

--apply-remote-conf
Obtain and apply additional configuration data from the extender. Following configuration is received:

- **calendar first time** - Aggregation time of the oldest calendar record the extender has.
- **calendar last time** - Aggregation time of the newest calendar record the extender has.

The time span is used to verify, whether signature extend request could be successfully performed. It must be noted that the described parameters are optional and may not be provided by the extender that you turn to. Use **--dump-conf** to view th provided configuration parameters.

--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. It must be noted that this value only affects KSI protocol PDUs.

--log *file*
Write **libksi** log to given file. Use '**-**' as file name to redirect log to *stdout*.

EXIT STATUS

See **ksi**(1) for more information.

EXAMPLES

In the following examples it is assumed that KSI service configuration (URLs, access credentials) options and trusted publications file are defined. See **ksi-conf**(5) for more information.

1 To extend a signature *sig.ksig* to the earliest available publication and save it as *ext.ksig*:

ksi extend -i *sig.ksig* **-o** *ext.ksig*

2 To extend a signature *sig.ksig* to specified publication (the publication string available from Financial Times, ISSN: 0307-1766, 2016-03-17 given as example):

ksi extend -i *sig.ksig* **-o** *ext.ksig* **--pub-str** *AAAAAA-CW45II-AAKWRK-F7FBNM-KB6FNV-DYYFW7-PJQN6F-JKZWBQ-3OQYZO-HCB7RA-YNYAGA-ODRL2V*

3 To extend a signature *sig.ksig* to specified calendar time *2015-05-05 00:00:00* and save it as *ext.ksig*:

ksi extend -i *sig.ksig* **-o** *ext.ksig* **-T** *"2015-05-05 00:00:00"*

4 To extend all signatures matching the pattern **.ksig* to specified publication (see https://twitter.com/Guardtime/status/799214699296346112) and save the output to the same directory where the input file is located (with altered file extension *ext.ksig*):

ksi extend **.ksig* **--pub-str** *AAAAAA-CYFJIA-AALGBS-ED4BKO-CMKY7Z-OMMBA5-NT6SJB-ZM677Q-JKCQAW-3OXD3O-OERGEO-DWJRYN*

5 Same as *Example 2*. In addition verify that the *extend to* time matches the calendar interval available in the extender:

ksi extend -i *sig.ksig* **-o** *ext.ksig* **--pub-str** *AAAAAA-CW45II-AAKWRK-F7FBNM-KB6FNV-DYYFW7-PJQN6F-JKZWBQ-3OQYZO-HCB7RA-YNYAGA-ODRL2V* **--apply-remote-conf**

6 Dump extender configuration in human-readable format to stdout:

ksi extend -X *http://example.gateway.com:8010/gt-extendingservice* **--dump-conf**

ENVIRONMENT

Use the environment variable **KSI_CONF** to define the default configuration file. See **ksi-conf**(5) for more information.

AUTHOR

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

SEE ALSO

ksi(1), **ksi-sign**(1), **ksi-verify**(1), **ksi-pubfile**(1), **ksi-conf**(5)