NAME

logksi extend - Extend KSI signatures in a log signature file.

SYNOPSIS

logksi extend <*logfile*> [**-o** <*out.logsig*>] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... [*more_options*]

logksi extend <*logfile*> [**-o** <*out.logsig*>] **-X** *URL* [**--ext-user** *user* **--ext-key** *key*] **-P** *URL* [**--cnstr** *oid=value*]... **--pub-str** *str* [*more_options*]

logksi extend --sig-from-stdin [**-o** <*out.logsig*>] [*more_options*]

DESCRIPTION

Finds the log signature file (<*logfile*>*.logsig* or <*logfile*>*.gtsig*) based on the specified log file <*logfile*> and extends KSI signatures in it to the desired publication. The log signature file is expected to be located in the same directory as the log file. Alternatively, if no <*logfile*> is specified, the log signature file may be read from *stdin*. To do that the **--sig-from-stdin** option should be used. If neither the <*logfile*> nor **--sig-from-stdin** option is given, help text is returned.

After the signatures are extended and the corresponding publication records are attached, the log signatures can be verified using publication-based verification where only trusted publications file or a publication string in printed media is needed to perform the verification. See **logksi-verify**(1) for details.

User must have access to KSI extending service and a trusted KSI publications file. By default the KSI signatures are extended to the earliest available publication. Use the option **--pub-str** to extend signatures to the publication denoted by the given publication string. Note that all KSI signatures present in the log signature file will be attempted to extend to the same publication. If for some reason the extending of at least one signature fails, none of the signatures are extended.

OPTIONS

<*logfile*>
: Name of the log file whose log signature file is to be extended. If <*logfile*> is specified, the **--sig-from-stdin** option cannot be used.

--sig-from-stdin
: Use to read the log signature file from *stdin*. If no output file is specified with **-o**, the result will be returned to *stdout*.

-o <*out.logsig*>
: Specify the name of the extended output log signature file; recommended file extension is *.logsig*. If not specified, the input file <*logfile*>*.logsig* or <*logfile*>*.gtsig* is modified. If the input file that is to be modified contains RFC3161 timestamps, the user must specify the **--enable-rfc3161-conversion** option to enable conversion, extending and replacing of RFC3161 timestamps with KSI signatures. The backup of the original log signature file will be saved to <*logfile*>*.logsig.bak*. If extending fails, the newly created <*logfile*>*.logsig* will be deleted and the original <*logfile*>*.logsig* will be restored from the backup file. If the output file name is explicitly specified, the existing file will always be overwritten and no backup file will be created. Use '-' as file name to redirect the output as a binary stream to *stdout*.

-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. All values from lower priority sources are ignored (see **logksi-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 the signatures to.

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

--enable-rfc3161-conversion
Enable conversion, extending and replacing of RFC3161 timestamps with KSI signatures. Note: this flag is not required if a different output log signature file name is specified with **-o** to avoid overwriting of the original log signature file.

-d Print detailed information about processes and errors to *stderr*. To make output more verbose increase debug level with **-dd** or **-ddd**. With debug level 1 a summary of log file is displayed. With debug level 2 a summary of each block and the log file is displayed. Debug level 3 will display the whole parsing of the log signature file. The parsing of *record hashes (r), tree hashes (.), final tree hashes (:)* and *meta-records (M)* is displayed inside curly brackets in following manner *{r.Mr..:}*. In case of a failure *(X)* is displayed and closing curly bracket is omitted.

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

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

EXIT STATUS

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

EXAMPLES

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

1 To extend the signatures in */var/log/secure.logsig* to the earliest available publication and save the file as */var/log/secureExt.logsig*:

logksi extend */var/log/secure* **-o** */var/log/secureExt.logsig*

2 To extend the signatures in */var/log/secure.logsig* to the specified publication (the publication string available from Financial Times, ISSN: 0307-1766, 2016-03-17 given as example) and save the result with the default name */var/log/secure.logsig*:

logksi extend */var/log/secure* **--pub-str** *AAAAAA-CW45II-AAKWRK-F7FBNM-KB6FNV-DYYFW7-PJQN6F-JKZWBQ-3OQYZO-HCB7RA-YNYAGA-ODRL2V*

3 To convert the RFC3161 timestamps in */var/log/secure.gtsig* to KSI signatures, extend them to the earliest available publication and save them in the original file */var/log/secure.gtsig*:

logksi extend */var/log/secure* **--enable-rfc3161-conversion**

ENVIRONMENT

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

AUTHOR

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

SEE ALSO

logksi(1), **logksi-extract**(1), **logksi-integrate**(1), **logksi-sign**(1), **logksi-verify**(1), **logksi-conf**(5)