



Certificate Manager for S/MIME Certificates

- iQ.Suite 9.x for Domino -

Command Line Tool "ntk_certmgr.exe"



Contents

1	Functionality	2
2	Procedure	2
3	Parameters.....	2
4	Important Notes for Using the Tool	4
5	About GROUP Technologies AG	7

1 Functionality

The Certificate Manager can be used to import existing certificates in the Certificates database (**g_cert.nsf** as of Version 8.0) or export certificates to the file system. This provides an easy way to distribute certificates. The tool also allows to import, export and delete certificate revocation lists (CRL).

For this purpose, iQ.Suite is delivered with the command line tool named **ntk_certmgr.exe**.

2 Procedure

After the iQ.Suite installation, the **ntk_certmgr.exe** command line tool is located in the Domino program directory; default: <drive>:\Lotus\Domino.

Proceed as follows to start **ntk_certmgr.exe** with the necessary parameters:

- Call with individual parameters
ntk_certmgr.exe <Working mode> <Certificates database path name> <CRL database path name> <Working directory> <Execution mode> <Sleeping time> <Logging mode> <LDAP Server> <LDAP port> <LDAP user> <LDAP password> <LDAP library>
- Call with a parameter file
ntk_certmgr.exe @paramfile.txt

Note: The format of the certificates to be imported must be "DER encoded binary X.509 (.CER)" or "Base-64 encoded X.509 (.CER)". The format of the CRLs to be imported must also be "DER encoded X.509 (.CRL)" or "Base-64 encoded X.509 (.CRL)".

3 Parameters

- **Working mode:**
 - Import:** Import certificates
 - Export:** Export certificates
 - CRL_IMPORT:** Import CRLs (remote and from local file system)
 - CRL_IMPORT_LOCAL:** Import CRLs (from local file system)
 - CRL_IMPORT_REMOTE:** Import CRLs (remote)
 - CRL_EXPORT:** Export CRLs
 - CRL_REMOVE_OLD:** Delete old CRL from CRL cache database

■ **Path name of the certificates database used:**

The path name consists of the entire path and the name of the database used. The name of the certificates database has to be specified without extension, i.e. for instance:
C:\Lotus\Data\iQSuiteData\g_cert

■ **Path name of the CRL database**

The path name consists of the entire path and the name of the database used. The name of the database used can be freely selected, for instance ... \crl.db. The file does not have to exist. It is automatically created when using the **ntk_certmgr.exe** command line tool.

■ **Working directory:**

This parameter is used to specify the complete path to the directory that contains the subdirectories and certificates needed for import/export.

e.g.: C:\Domino\iQSuite\smime\Import
or C:\Domino\iQSuite\smime\Export
or C:\Domino\iQSuite\smime\crl_import
or C:\Domino\iQSuite\smime\crl_export

■ **Execution mode:**

"CMDLINE"

In CMDLINE mode, the tool is run only once and the certificates or CRLs are imported or exported, depending on the parameter settings.

In future iQ.Suite versions it is planned to also provide the Certificate Manager as Server add-in.

■ **Sleeping time:**

Sets the interval in seconds between individual runs.

■ **Logging mode**

"NORMAL" or "SILENT"

In **SILENT** mode, the only information logged is that CertMgr is started and ended.

In **NORMAL** mode, some additional information is also logged. Logging information is output to the server console.

■ **LDAP server**

Specifies the name or IP address of the server from which the CRLs are to be imported. If this parameter is not to be used, a zero has to be entered instead.

■ **LDAP port**

Specifies the port to be used to address the LDAP server for importing the CRLs. If this parameter is not to be used, a zero has to be entered instead.

■ **LDAP user name**

Name of the LDAP user to be used to address the LDAP server for importing the CRLs. If this parameter is not to be used, a zero has to be entered instead.

LDAP password

Password of the LDAP user to be used to address the LDAP server for importing the CRLs. If this parameter is not to be used, a zero has to be entered instead.

LDAP library

This parameter allows to specify an alternative LDAP library or DLL to be used for LDAP access. If this parameter is not to be used, a zero has to be entered instead.

4 Important Notes for Using the Tool

- All of the parameters must be set.
- It's possible to use a Domino program document for call of Command Line tool. The program name is **tk_certmgr**.
- Path names must be absolute.
- The certificates database must exist; where required, the CRL database is automatically created.
- It's possible to use absolute path names for call of parameter files, e.g.
`ntk_certmgr.exe @C:\Temp\param.txt`
- Under the working directory to be configured, the following subdirectories must exist for both importing and exporting certificates:
 - Trusted**
 - Nottrusted**
 - Path**

This yields the following paths (example):

Import:

- C:\Domino\iQSuite\smime\Import\Trusted
- C:\Domino\iQSuite\smime\Import\Nottrusted
- C:\Domino\iQSuite\smime\Import\Path

Export:

- C:\Domino\iQSuite\smime\Export\Trusted
- C:\Domino\iQSuite\smime\Export\Nottrusted
- C:\Domino\iQSuite\smime\Export\Path

This is imperatively required, as the certificates to be exported are copied to the file system according to their trust status within the certificates database.

For instance, a certificate explicitly trusted in the certificates database will be exported to the subdirectory named "Trusted".

When imported, the directory where the certificates are located is used to set the trust state assigned to the certificates after having been successfully imported into the certificates database.

For instance, a certificate located in the directory named "Nottrusted" will be set to "explicitly not trusted" in the database.

- A special case occurs when root certificates to be imported are located in the directory "Path":

For root certificates, the trust status cannot be determined from the path, as there are no higher-ranking certificates. In such a situation, the root certificates are set to "explicitly trusted" when imported into the certificates database.
- All certificates imported are set to "Active" in the certificates database.
- Only "Active" certificates can be exported.
- Once successfully imported, the certificates are deleted from the file system.
- The filename used for export is formed from the first 50 characters of the SubjectDN and a unique hash value calculated separately for each certificate. To ensure that the filename used does not contain forbidden characters, any such character is replaced with an underscore ("_"). Under normal circumstances, the filename will not exactly match the SubjectDN but it will be sufficiently similar to reliably identify the certificate.
- If the **CRL_IMPORT_LOCAL** working mode is selected to import CRLs, the local CRLs will be imported from the CRL Import directory. After having been imported, the lists are deleted from the file system. Only current CRLs are taken into account (expired CRLs are ignored).
- If the **CRL_IMPORT_REMOTE** working mode is selected to import CRLs, the lists are imported via LDAP, FTP or HTTP. For this to happen, the certificates located in the certificates database must contain the corresponding distribution point information, i.e. from where CRLs can be copied remotely. Again, only current CRLs are taken into account. Please make sure the corresponding ports are made available at the firewall.
- If the **CRL_IMPORT** working mode is selected to import CRLs, the lists are first imported according to the **CRL_IMPORT_LOCAL** working mode and then according to the **CRL_IMPORT_REMOTE** working mode.
- After one or more CRLs have been imported, the system always performs a revocation check, i.e. all certificates located in the certificates database are checked for matching entries in one of the CRLs. If that is the case, the corresponding certificate is set to "not trusted" and the "Revoked" field is written with a "1" in the certificates document. If the certificate is not found in any of the CRLs, the issuer path is checked. All issuer certificates are treated in the same way.

- CRLs are always exported to the directory configured, in two formats: as readable file with the name/extension "...decoded.txt" and as binary file with the name/extension "...encoded.crl".
- When old CRLs are deleted from the CRL database in **CRL_REMOVE_OLD** working mode, no S/MIME jobs may be active. Otherwise, the MailGrabber must be stopped and restarted after having run the Certificate Manager.
- A separate log file is written for each working mode:
 - Importing certificates: ***iQSuite_cert_import.out***
 - Exporting certificates: ***iQSuite_cert_export.out***
 - Importing CRLs: ***iQSuite_crl_import.out***
 - Exporting CRLs: ***iQSuite_crl_export.out***
 - Deleting old CRLs from the CRL cache database: ***iQSuite_crl_remove_old.out***

5 About GROUP Technologies AG

GROUP Technologies AG is a world leader in E-mail Lifecycle Management. The company's fully integrated iQ.Suite products ensure efficient security and effective organization of e-mail, from encryption, virus protection, and spam filters to e-mail classification and secure archiving.

The iQ.Suite is modular, fully scalable, and offers a high degree of investment security. The modules are completely server-based, can be centrally administered at a low cost, and are available for Lotus Domino, Microsoft Exchange and SMTP platforms.

With the iQ.Suite, companies can reduce costs, optimize the performance of their e-mail environment, and increase productivity. GROUP's clients include many well-known companies such as Deutsche Bank, Ernst & Young, Honda, Heineken, and Miele. More than six million users and 2,000 companies worldwide protect and organize their systems with GROUP Technologies products.

GROUP Technologies AG is headquartered in Karlsruhe. It maintains a subsidiary in the USA, and distributes its products internationally, both directly and through partner companies.

www.group-technologies.com

© 2006 GROUP Technologies

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warranty. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments.

The information contained in this documentation deals with issues as assessed by GROUP Technologies AG at the time of publication. As GROUP Technologies AG is bound to react to changing market requirements, this document by no means represents an obligation by GROUP Technologies AG and GROUP cannot guarantee the correctness of the information presented in this document after its publication.

This documentation is intended for information purposes only. GROUP Technologies AG hereby excludes any warranty, express or implied, for this document. GROUP Technologies AG is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

All product or company names in this document may be protected brand names of their respective owners.

GROUP Technologies

Ottostrasse 4

76227 Karlsruhe / Germany

Phone +49(0)721-4901-0

Fax +49(0)721-4901-199

info.de@group-technologies.com

www.group-technologies.com



North American Headquarters

GROUP Technologies

120 Quarry Drive, Suite B214

Milford, MA 01754/USA

Phone +1 508-473-3332

Phone 877-476-8755 (US and Canada)

Fax +1 508-473-9940

info.us@group-technologies.com

www.group-technologies.com