



Certificate Manager

Importing and Exporting S/MIME Certificates and Certificate Revocation Lists for iQ.Suite Lotus Notes and iQ.Suite Exchange

Document version: 2.0

Contents

1	About GROUP Technologies AG	2
2	Brief Description	3
3	Using Certificates	4
3.1	Importing Certificates	4
3.1.1	Procedure Under LND	4
3.1.2	Procedure Under Exchange	5
3.2	Exporting Certificates	5
3.2.1	Procedure Under LND	6
3.2.2	Procedure Under Exchange	6
4	Using Certificate Revocation Lists (CRLs)	7
4.1	Importing Certificate Revocation Lists	7
4.1.1	Example: Importing Certificate Revocation Lists	7
4.2	Exporting Certificate Revocation Lists	8
4.3	Deleting Certificate Revocation Lists	9
5	Revocation Check	9
6	Starting the Certificate Manager	10
6.1	Parameters	10
6.2	Calling Modes	10

1 About GROUP Technologies AG

GROUP Technologies AG is the provider of solutions for process-oriented, secure and legally conforming email management. Regardless of size, companies can centrally incorporate email communication into business processes, in accordance with current legal requirements and operative demands.

The company's core solutions – *GROUP MailSecure* and *GROUP MailArchive* – enable processing, saving and managing of emails, from creation to deletion. This includes virus and spam protection, data and content control, encryption, classification, automated archiving as well as intelligent retrieval of emails and their attachments. This not only ensures the highest possible level of security for company information but also simultaneously increases the efficiency of the entire organization. In addition, companies and their decision makers are protected from sanctions resulting from infractions of other regulations concerning privacy and data protection or labeling obligations.

The company's customer base includes more than three quarters of the German Sparkasse and Volksbank Groups as well as many international companies such as ABN AMRO, Allianz, Deutsche Bank, Ernst & Young, Honda, Heineken and Miele. Currently, well over three million users are relying on the company's know-how and solutions.

www.group-technologies.com

2 Brief Description

The Certificate Manager (CM) is a free-of-charge iQ.Suite feature, which allows to distribute certificates as well as certificate revocation lists (CRL) in a most easy and convenient way.

The Certificate Manager is primarily used exchange certificates as well as certificate revocation lists (via import or export) between iQ.Suite and the local file system.

The Certificate Manager is provided as exe file. Call parameters are used to control in which mode the Certificate Manager is run. Depending on the mode set, the certificates or certificate revocation lists are either imported or exported.

Following an import of a certificate revocation list, the system automatically performs a revocation check. Thus, the certificates are reclassified as trustworthy or untrustworthy each time a new CRL is imported. As CRLs tend to become outdated over time, a parameter allows to have old revocation lists automatically deleted after a specific period of time.

Basically, the functioning of the iQ.Suite Certificate Manager is very similar under Lotus Notes and Exchange, with only minor differences in a limited number of points. The description below of the Certificate Manager functionalities applies to Lotus Notes as of version 9.0 or Exchange as of version 5.

After having installed iQ.Suite, a command line tool is provided to start the Certificate Manager:

- For Lotus Notes Domino: the **ntk_certmgr.exe** file in the Domino program directory under `<path>\Lotus\Domino`.
It is possible to use the command line tool in Domino program documents. The program name is **tk_certmgr**.
- For Exchange: the **tk_certmgr.exe** file in the iQ.Suite directory under `<path>\iQ.Suite\Bin\smime`.

Alternative: It is also possible to use parameter files via an absolute path, e.g.
`(n)tk_certmgr.exe@ C:\temp\param.txt.`

3 Using Certificates

3.1 Importing Certificates

Existing certificates can be imported into iQ.Suite through the file system. This requires that the certificates be located in a specific import directory within the file system (as set in the configuration).

Note: The format of the certificates to be imported has to be “DER encoded binary X.509 (.CER)” or “Base-64 encoded X.509 (.CER)”.

3.1.1 Procedure Under LND

Under LND, the imported certificates are stored in the certificate database (g_cert.nsf) within iQ.Suite. The database is displayed under **Crypt -> S/MIME Certificates -> Active by Issuer, Active by Email address and All by Status**.

Proceed as follows:

1. In the file system, manually create an import folder with the subdirectories “trusted”, “nottrusted” and “path”. These subdirectories are absolutely necessary. When imported into the certificate database, the folder where the certificates are located, determines the trust status assigned to the certificates. For instance, a certificate located in the “Nottrusted” folder will be stored in the iQ.Suite certificate database under “Explicitly not trustworthy”.
Therefore, the following paths (examples) need to be specified when configuring the Certificate Manager:
 - C:\Domino\iQSuite\smime\Import\Trusted
 - C:\Domino\iQSuite\smime\Import\Nottrusted
 - C:\Domino\iQSuite\smime\Import\Path
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). Select **IMPORT** as working mode.
3. The “iQSuite_cert_import.out” log file is used to log the certificate import procedure. It is written to the iQ.Suite data directory.
4. If imported successfully, the certificates are stored in the certificate database with the status set to “Active” and deleted from the file system.

Note: For root certificates located in the “Path” directory after having been imported, the following exception applies: The trust status of root certificates cannot be derived from the path, as there are no higher-ranking certificates. In this case, once imported, root certificates are explicitly trusted in the certificate database.

3.1.2 Procedure Under Exchange

Under Exchange, the imported certificates are stored in a certificate database that is not displayed in the iQ.Suite front-end. In this case, the certificate database corresponds to a cache database where the certificates are stored. Within this certificate database, the trust status of the certificates cannot be changed.

When imported, root certificates are systematically considered trustworthy (status “Trusted”). As the associated certificates get their status from the path, the lower-ranking certificates are automatically trusted as well.

Proceed as follows:

1. Make sure that all certificates to be imported are located in the file system folder that has been specified in the configuration. The paths to the certificates are specified when configuring the Certificate Manager.
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). Select **IMPORT** as working mode.
3. The “iQSuite_cert_import.out” log file is used to log the certificate import procedure. It is written to the directory where the Certificate Manager is located.
4. If imported successfully, the certificates are automatically classified as trustworthy, stored in the certificate database, and finally deleted from the file system.

3.2 Exporting Certificates

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.

Note: Certificates are exported in the format “DER encoded binary X.509 (.CER)”.

3.2.1 Procedure Under LND

The certificates stored in the certificate database (g_cert.nsf) under **Crypt -> S/MIME Certificates** can be exported to the local file system. Only “Active” certificates are taken into account.

Proceed as follows:

1. In the file system, manually create an export folder with the subdirectories “trusted”, “nottrusted” and “path”. These subdirectories are absolutely necessary. When exported to the file system, trust status assigned to the certificates within the certificate database determines the folder where the certificates will be exported to. For instance, a certificate explicitly trusted in the certificate database will be exported to the “Trusted” folder.
Therefore, the following paths (examples) need to be specified when configuring the Certificate Manager:
 - C:\Domino\iQSuite\smime\Export\Trusted
 - C:\Domino\iQSuite\smime\Export\Nottrusted
 - C:\Domino\iQSuite\smime\Export\Path
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). Select **EXPORT** as working mode.
3. The “iQSuite_cert_export.out” log file is used to log the certificate export procedure. It is written to the iQ.Suite data directory.

3.2.2 Procedure Under Exchange

Under Exchange, the certificates to be exported are stored in a certificate database that is not displayed in the iQ.Suite front-end. In this case, the certificate database corresponds to a cache database where the certificates are stored. Within this certificate database, the trust status of the certificates cannot be changed.

1. Make sure the file system folder to where the certificates are to be exported has been created. The directory path to this folder has to be specified in the configuration.
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). Select **EXPORT** as working mode.
5. The “iQSuite_cert_export.out” file is used to log the certificate export procedure. It is written to the directory where the Certificate Manager is located.

Note: 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.

4 Using Certificate Revocation Lists (CRLs)

4.1 Importing Certificate Revocation Lists

Similarly to the certificate import procedure, it is also possible to import certificate revocation lists into iQ.Suite. Under both platforms, the import procedure uses a CRL database. Under Lotus Notes Domino this is the g_certs.nsf database, under Exchange it is the cache database. The name of the database is set in the configuration.

The following options are available when importing certificate revocation lists:

- Local CRL Import

If Local CRL Import is selected, the existing local certificate revocation lists are imported into iQ.Suite. The CRLs need to be located in a specific import folder within the file system (to be set in the configuration). After having been imported, the lists are deleted from the file system.

- Remote CRL Import

If Remote CRL Import is selected, the certificate revocation lists provided on external websites are imported remotely. To this end, the system first checks the certificates stored in the iQ.Suite certificate database. If the certificates contain distribution point information (DPI) on the external websites where CRLs are available (complete path and full name required), remote access to the certificate revocation lists stored there is possible. The CRLs are imported into the CRL database using LDAP, LDAPS, LDAPi, FTP or HTTP.

As a general rule, only current CRLs with the file extension “.crl” are taken into account. Expired CRLs (for which a new CRL should exist) are not imported. When import is complete, the system performs a revocation check, refer to [Revocation Check](#).

Note: The format for CRLs to be imported has to be “DER encoded X.509 (.CRL)” or “Base-64 encoded X.509 (.CRL)”.

4.1.1 Example: Importing Certificate Revocation Lists

Normally, the Certificate Manager is first used for a local CRL import and then for a remote CRL import. This sequence of operations is described below:

1. Make sure that all CRLs to be imported are stored in the files system folder set in the configuration and have the file extension “.crl”.
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). To perform a local CRL import and then a remote CRL import, select the **CRL_IMPORT** parameter under **Working mode**.

4. The local CRLs are imported into the CRL database and deleted from the file system (Local CRL Import).
5. The certificates stored in the certificate database are checked for specific information (DPI). If the necessary information is available, the system establishes a connection to the external certificate revocation lists and then imports them into the CRL database (Remote CRL Import).
3. A separate log file is written for each **working mode**.
4. When import is complete, the system performs a revocation check, refer to [Revocation Check](#).

Note: To perform a local CRL import only, select the **CRL_IMPORT_LOCAL** parameter under **Working mode**. To perform a remote CRL import only, select the **CRL_IMPORT_REMOTE** parameter.

4.2 Exporting Certificate Revocation Lists

The certificate revocation lists stored in the CRL database can be exported to the file system. To this end, the CRLs are exported to a specific folder set in the configuration.

Proceed as follows:

1. Make sure all of the certificate revocation lists to be exported are included in the CRL database and have the file extension “.crl”.
2. Start the Certificate Manager as described under [Starting the Certificate Manager](#). To perform a CRL export, select the **CRL_EXPORT** parameter under **Working mode**.
3. The “iQSuite_crl_export.out” file is used to log the CRL export procedure. Under Lotus Notes Domino it is written to the iQ.Suite data directory, under Exchange to the directory where the Certificate Manager is located.

Note: To avoid overwriting in case the CRL is exported again, the filename of the exported CRL is made up of an abbreviated form of the IssuerDN (issuer of the CRL) and a unique hash value.

CRLs are always exported to the directory configured, in two formats:

- as readable file with the extension “...decoded.txt”
- as binary file with the extension “...encoded.crl”.

4.3 Deleting Certificate Revocation Lists

Outdated certificate revocation lists are complemented with new ones. The information as to when a new CRL is published is provided within the CRL itself. To delete outdated certificate revocation lists from the CRL database, set the working mode to **CRL_REMOVE_OLD**. The deletion procedure is logged in the "iQSuite_crl_remove_old.out" file.

Note: Before setting the working mode to **CRL_REMOVE_OLD** be sure that no S/MIME jobs are active.

5 Revocation Check

When a CRL import is complete (either local or remote), the system performs a revocation check. The serial numbers of all certificates located in the iQ.Suite certificate database are checked for matching entries in one of the certificate revocation lists in the CRL database. Certificates found in a CRL are handled as follows:

- Under LND: The certificates are set to "Not trusted". The "Revoked" field is set to "1" and written to the certificate document.
- Under Exchange: The certificates are deleted.

If the certificate is not listed in any of the CRLs, the issuer path is checked. All issuer certificates are checked in the same way and, where required, set to "Revoked" or deleted from the certificate database as described above. Whenever a "Revoked" field set to "1" is found in a certificate, checking the issuer path is aborted.

Note: The "tk_smime" is neither used for the revocation check nor for handling certificate revocation lists. The Certificate Manager works autonomously. If a certificate has been classified as untrustworthy by the Certificate Manager, this certificate will not be used by "tk_smime" for subsequent e-mail processing.

6 Starting the Certificate Manager

6.1 Parameters

To start the Certificate Manager run the **(n)tk_certmgr.exe** file using one of the two methods below:

- Using a parameter file, e.g. “(n)tk_certmgr.exe @paramfile.txt” :
The name of this file is freely selectable. Each line must contain one parameter only.
- From the command line:
“(nt)tk_certmgr.exe <working mode> <path name of the certificate database> <path name of the CRL database> <working directory> <execution mode> <sleeping time> <logging mode> <LDAP server> <LDAP port> <LDAP user> <LDAP password> <LDAP library>“

In both cases, enter the parameters in the order above and use absolute path names. All of the parameters have to be set. Be sure to set the **<Working mode>** parameter correctly as this parameter sets the action performed by the Certificate Manager, e.g. importing certificates or exporting certificate revocation lists.

6.2 Calling Modes

The following parameters are available when calling the Certificate Manager. All of the parameters have to be set.

- **<Working mode>**:
 - **IMPORT**: Importing certificates
 - **EXPORT**: Exporting certificates
 - **CRL_IMPORT_LOCAL**: Importing CRLs from the local file system.
The local CRLs located in the CRL import folder are imported, after which the CRLs are deleted from the file system. Please note that only current CRLs are taken into account.
 - **CRL_IMPORT_REMOTE**: Importing CRLs (remote).
The CRLs are imported via LDAP, FTP or HTTP. This only happens if the certificates stored in the certificate database contain appropriate distribution point information, i.e. from where the CRLs can be copied. Again, only current CRLs are taken into account. The corresponding default ports (LDAP, FTP, http) have to be enabled at the firewall.

- **CRL_IMPORT:** Importing CRLs (local and remote).
The CRLs are first imported according to the **CRL_IMPORT_LOCAL** working mode, and then according to the **CRL_IMPORT_REMOTE** mode.
- **CRL_EXPORT:** Exporting CRLs
- **CRL_REMOVE_OLD:** Deleting old CRLs from the CRL database. Under LND, make sure that no S/MIME jobs are enabled. Otherwise, the MailGrabber would have to be stopped and restarted after the Certificate Manager has been closed again.
- **<Path name of the certificate database>:**
Enter the path name of the certificate database used. The path name includes the complete path and the filename of the database used.
 - For LND: The name of the certificate database has to be specified without extension, e.g.: `C:\Lotus\Data\iQSuiteData\g_cert`
 - For Exchange: The name of the certificate database is freely selectable, e.g.: `...\certs.db`
- **< Path name of the CRL database>:**
Enter the path name of the CRL database used. The path name includes the complete path and the filename of the database used.
 - For LND: The name of the CRL database has to be specified without extension, e.g.: `C:\Lotus\Data\iQSuiteData\g_cert`
 - For Exchange: The name of the CRL database (cache database) is freely selectable, e.g.: `...\certs.db`
- **<Working directory>:**
Enter the complete path to the directory that contains the subdirectories and certificates required for import or 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>:**
To import or export the certificates or CRLs (as configured), you need to specify the execution mode:
 - CMDLINE: The **exe file** is executed once from the command line.
 - LND only: SRVTASK: The **exe file** is executed once as server add-in.
- **<Sleeping time>:**
Period of time between runs (to be set in seconds).
- **<Logging mode>:**
 - NORMAL
Standard logging by the Certificate Manager. The information logged is output to the server console.

- SILENT

Reduced logging. The only information logged are the Certificate Manager start/end times.

- **<LDAP server>:**

Enter the name or IP address of the LDAP server to be used for importing the CRLs. If not required, set the parameter to "0".

- **<LDAP port>:**

Enter the port to be used to address the LDAP server for importing the CRLs. If not required, set the parameter to "0".

- **<LDAP user>:**

Enter the name of the LDAP user to be used to address the LDAP server for importing the CRLs. If not required, set the parameter to "0".

- **<LDAP password>:**

Enter the password of the LDAP user to be used to address the LDAP server for importing the CRLs. If not required, set the parameter to "0".

- **<LDAP library>:**

Enter an alternative LDAP library or DLL to be used for LDAP access. If not required, set the parameter to "0".

© 2008 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.



European Headquarters:
GROUP Technologies AG
MesseTurm
60308 Frankfurt
Deutschland

Head Office:
Fon: +49 (0)69-789-8819-0
Fax: +49 (0)69-789-8819-99

Sales:
Fon: +49 (0)721-4901-0
Fax: +49(0)721-4901-199

Hotline:
Fon +49(0)721-4901-112
Fax +49(0)721-4901-1922

hotline@group-technologies.com
info@group-technologies.com
<http://www.group-technologies.com>

In the US:
GROUP Technologies
c/o Relavis Corporation
40 Wall Street
New York, New York 10005
USA

Head Office:
Fon: +1 212-995-2900
Fax: +1 212-995-2206

Sales:
Fon: +1 212-995-2900

Hotline:
Fon: +1 877-476-8755
(US and Canada Only)

us.support@group-technologies.com
info@group-technologies.com
<http://www.group-technologies.com>