



Zertifikatsmanager

**Import und Export von S/MIME-Zertifikaten
und Zertifikatssperrlisten für
iQ.Suite Lotus Notes und iQ.Suite Exchange**

Dokumentversion: 2.0

Inhalt

1	Über GROUP Technologies AG	2
2	Kurzbeschreibung	3
3	Umgang mit Zertifikaten	4
3.1	Zertifikate importieren	4
3.1.1	Vorgehensweise unter LND	4
3.1.2	Vorgehensweise unter Exchange	5
3.2	Zertifikate exportieren	5
3.2.1	Vorgehensweise unter LND	6
3.2.2	Vorgehensweise unter Exchange	6
4	Umgang mit Zertifikatssperrlisten (CRLs)	7
4.1	Zertifikatssperrlisten importieren	7
4.1.1	Beispiel: Zertifikatssperrlisten importieren	8
4.2	Zertifikatssperrlisten exportieren	8
4.3	Zertifikatssperrlisten löschen	9
5	Revocation Check	9
6	Zertifikatsmanager starten	10
6.1	Parameteranruf	10
6.2	Modi des Parameteranrufs	10

1 Über GROUP Technologies AG

Die GROUP Technologies AG ist der Lösungsanbieter für prozessorientiertes, sicheres und gesetzeskonformes E-Mail-Management. Unabhängig von ihrer Größe, sind Unternehmen damit in der Lage, ihre E-Mail-Kommunikation in Übereinstimmung mit den aktuellen gesetzlichen Anforderungen und betrieblichen Vorgaben zentral in die Geschäftsprozesse einzubinden.

Die Kernlösungen *GROUP MailSecure* und *GROUP MailArchive* ermöglichen das Verarbeiten, Speichern und Verwalten von E-Mails – von deren Entstehung bis zur Löschung. Dazu zählen Viren- und Spamschutz, Daten- und Inhaltskontrolle, Verschlüsselung, Klassifizierung, automatisierte Speicherung und intelligente Rückgewinnung von E-Mails und deren Anlagen. Dadurch wird nicht nur der höchstmögliche Sicherheitsstandard für Unternehmensdaten erzielt, sondern zugleich auch die Effizienz der gesamten Organisation gesteigert. Zusätzlich werden Unternehmen und ihre Entscheidungsträger vor Bußgeldern bewahrt, die bei Verstößen gegen unter anderem datenschutzrechtliche Vorschriften oder Kennzeichnungspflichten drohen.

Zu den Kunden von GROUP Technologies zählen neben mehr als drei Viertel der Sparkassen und Volksbanken in Deutschland, unter anderem auch zahlreiche internationale Unternehmen wie ABN AMRO, Allianz, Deutsche Bank, Ernst & Young, Honda, Heineken und Miele. Mehr als drei Millionen User bauen bereits auf die Expertise des Lösungsanbieters.

www.group-technologies.com

2 Kurzbeschreibung

Der Zertifikatsmanager (engl. Certificate Manager, kurz: CM) ist eine kostenlose Funktion der iQ.Suite und ermöglicht Ihnen, Zertifikate sowie Zertifikatssperrlisten auf einfachem Weg zu verteilen.

Mit dem Zertifikatsmanager können Zertifikate sowie Zertifikatssperrlisten via Import oder Export zwischen der iQ.Suite und dem lokalen Dateisystem ausgetauscht werden.

Der Zertifikatsmanager ist als exe-Datei gelöst. Durch den Aufruf mit bestimmten Parametern wird gesteuert, in welchem Modus der Zertifikatsmanager betrieben wird. In Abhängigkeit des Modus wird ein Import oder Export von Zertifikaten bzw. Zertifikatssperrlisten (engl. Certificate Revocation Lists, kurz: CRL) durchgeführt.

Nach dem Import einer Zertifikatssperrliste wird automatisch ein Revocation Check durchgeführt. So werden Zertifikate nach jedem Import einer neuen CRL als vertrauenswürdig oder nicht vertrauenswürdig klassifiziert. Da einmal importierte CRLs nach einiger Zeit veralten, steht zudem ein Parameter zur Löschung veralteter Sperrlisten zur Verfügung.

Die Funktionsweise des Zertifikatsmanagers der iQ.Suite ist unter Lotus Notes und Exchange ähnlich und unterscheidet sich nur in wenigen Punkten. Der nachfolgend beschriebene Funktionsumfang des Zertifikatsmanagers kann unter Lotus Notes ab Version 9.0, unter Exchange ab Version 5 eingesetzt werden.

Zum Start des Zertifikatsmanagers steht nach der Installation der iQ.Suite ein Command Line Tool zur Verfügung:

- Bei Lotus Notes Domino die Datei **ntk_certmgr.exe** im Domino-Programmverzeichnis unter `<path>\Lotus\Domino`.
Die Verwendung des Command Line Tools in Domino Programmdokumenten ist möglich. Der Programmname ist **tk_certmgr**.
- Bei Exchange die Datei **tk_certmgr.exe** im iQ.Suite-Verzeichnis unter `<path>\iQ.Suite\Bin\smime`.

Alternative: Die Verwendung von Parameterdateien ist auch über absolute Pfade möglich, z.B. `(n)tk_certmgr.exe@ C:\temp\param.txt`.

3 Umgang mit Zertifikaten

3.1 Zertifikate importieren

Bereits vorhandene Zertifikate können über das Dateisystem in die iQ.Suite importiert und dort verwendet werden. Dazu müssen die Zertifikate in einem bestimmten Import-Verzeichnis innerhalb des Dateisystems abgelegt sein, welches durch die Konfiguration vorgegeben ist.

Hinweis: Das Format der zu importierenden Zertifikate muss „DER encoded binary X.509 (.CER)“ oder „Base-64 encoded X.509 (.CER)“ sein.

3.1.1 Vorgehensweise unter LND

Unter LND werden die importierten Zertifikate in der Zertifikatsdatenbank (g_cert.nsf) innerhalb der iQ.Suite abgelegt. Diese wird unter **Crypt -> S/MIME Zertifikate -> Aktive nach Aussteller, Aktive nach E-Mail-Adresse** und **Alle nach Status** angezeigt.

Gehen Sie wie folgt vor:

1. Legen Sie im Dateisystem manuell einen Import-Ordner mit den Unterverzeichnissen „trusted“, „nottrusted“ und „path“ an. Diese Unterverzeichnisse sind zwingend erforderlich. Beim Import entscheidet der Ordner, in dem die Zertifikate liegen, über den Vertrauensstatus, den die Zertifikate nach erfolgreichem Import in der Zertifikatsdatenbank erhalten. Beispielsweise wird ein Zertifikat, das im Ordner „Nottrusted“ abgelegt ist, in der iQ.Suite im Bereich „explizit nicht vertrauenswürdig“ der Zertifikatsdatenbank eingepflegt.
Es ergeben sich demnach beispielhaft die folgenden Pfade, die bei der Konfiguration des Zertifikatsmanagers angegeben werden müssen:
 - C:\Domino\iQSuite\smime\Import\Trusted
 - C:\Domino\iQSuite\smime\Import\Nottrusted
 - C:\Domino\iQSuite\smime\Import\Path
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) angegeben. Wählen Sie als Arbeitsmodus **IMPORT** aus.
3. Die Logdatei „iQSuite_cert_import.out“ protokolliert den Zertifikatsimport und wird in das iQSuite DataDir geschrieben.
4. Die Zertifikate werden bei erfolgreichem Import mit dem Status „Aktiv“ in die Zertifikatsdatenbank eingepflegt und aus dem Dateisystem gelöscht.

Hinweis: Bei Root-Zertifikaten, die während des Imports im Verzeichnis „Path“ liegen, gilt folgende Ausnahme: Der Vertrauensstatus von Root-Zertifikaten kann nicht aus dem Pfad ermittelt werden, da keine übergeordneten Zertifikate existieren. In einer solchen Situation wird den Root-

Zertifikaten während des Imports das explizite Vertrauen innerhalb der Zertifikatsdatenbank ausgesprochen.

3.1.2 Vorgehensweise unter Exchange

Unter Exchange wird für den Zertifikatsimport eine Zertifikatsdatenbank eingesetzt, die nicht im Frontend der iQ.Suite angezeigt wird. Die Zertifikatsdatenbank entspricht in diesem Fall einer Cache-Datenbank, in der die Zertifikate abgelegt werden. Der Vertrauensstatus eines Zertifikats innerhalb dieser Zertifikatsdatenbank kann nicht beeinflusst werden.

Beim Import werden Root-Zertifikate grundsätzlich als vertrauenswürdig eingestuft (Status „Trusted“). Da die zugehörigen Zertifikate ihren Status aus dem Pfad beziehen, wird den untergeordneten Zertifikaten automatisch ebenfalls vertraut.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass alle zu importierenden Zertifikate in dem durch die Konfiguration vorgegebenen Ordner innerhalb des Dateisystems abgelegt sind. Die Pfade zu den Zertifikaten werden bei Konfiguration des Zertifikatsmanagers angegeben.
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) beschrieben. Wählen Sie als Arbeitsmodus **IMPORT** aus.
3. Die Logdatei „iQSuite_cert_import.out“ protokolliert den Zertifikatsimport und wird in dem Verzeichnis erzeugt, in dem sich der Zertifikatsmanager befindet.
4. Nach erfolgreichem Import werden die Zertifikate automatisch als vertrauenswürdig klassifiziert, in der Zertifikatsdatenbank abgelegt und aus dem Dateisystem gelöscht.

3.2 Zertifikate exportieren

Der für den Export verwendete Dateiname wird aus den ersten 50 Zeichen des SubjectDN, sowie einem eindeutigen, nur für das jeweilige Zertifikat ermittelten Hash-Wert gebildet. Damit ein Dateiname verwendet wird, der keine verbotenen Zeichen enthält, wird er vor seiner Verwendung entsprechend bereinigt und verbotene Zeichen durch „_“ (Unterstrich) ersetzt. Im Normalfall wird somit der Dateiname nicht exakt dem SubjectDN entsprechen. Durch eine hinreichende Ähnlichkeit wird eindeutig zu erkennen sein, um welches Zertifikat es sich handelt.

Hinweis: Zertifikate werden im Format „DER encoded binary X.509 (.CER)“ exportiert.

3.2.1 Vorgehensweise unter LND

Die in der Zertifikatsdatenbank (g_cert.nsf) unter **Crypt -> S/MIME Zertifikate** abgelegten Zertifikate können in das lokale Dateisystem exportiert werden. Hierbei werden lediglich „aktive“ Zertifikate berücksichtigt.

Gehen Sie wie folgt vor:

1. Legen Sie im Dateisystem manuell einen Import-Ordner mit den Unterverzeichnissen „trusted“, „nottrusted“ und „path“ an. Diese Unterverzeichnisse sind zwingend notwendig, da die Zertifikate beim Export – entsprechend ihrem Vertrauensstatus innerhalb der Zertifikatsdatenbank – ins Dateisystem exportiert werden. Beispielsweise wird ein Zertifikat, dem in der Zertifikatsdatenbank das explizite Vertrauen ausgesprochen wurde, in den Ordner „Trusted“ exportiert.
Es ergeben sich demnach beispielhaft die folgenden Pfade, die bei der Konfiguration des Zertifikatsmanagers angegeben werden müssen:
 - C:\Domino\iQSuite\smime\Export\Trusted
 - C:\Domino\iQSuite\smime\Export\Nottrusted
 - C:\Domino\iQSuite\smime\Export\Path
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) angegeben. Wählen Sie als Arbeitsmodus **EXPORT** aus.
3. Die Logdatei „iQSuite_cert_export.out“ protokolliert den Zertifikatsexport und wird in das iQSuite DataDir geschrieben.

3.2.2 Vorgehensweise unter Exchange

Unter Exchange wird für den Zertifikatsexport eine Zertifikatsdatenbank eingesetzt, die nicht im Frontend der iQ.Suite angezeigt wird. Die Zertifikatsdatenbank entspricht in diesem Fall einer Cache-Datenbank, in der die Zertifikate abgelegt werden. Der Vertrauensstatus eines Zertifikats innerhalb dieser Zertifikatsdatenbank kann nicht beeinflusst werden.

1. Stellen Sie sicher, dass im Dateisystem der Ordner angelegt wurde, in den die Zertifikate exportiert werden sollen. Der Verzeichnispfad des Ordners muss in der Konfiguration angegeben werden.
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) angegeben. Wählen Sie als Arbeitsmodus **EXPORT** aus.
5. Die Logdatei „iQSuite_cert_export.out“ protokolliert den Zertifikatsexport und wird in dem Verzeichnis erzeugt, in dem sich der Zertifikatsmanager befindet.

Hinweis: Der für den Export verwendete Dateiname wird aus den ersten 50 Zeichen des SubjectDN, sowie einem eindeutigen, nur für das jeweilige Zertifikat ermittelten Hash-Wert gebildet. Damit ein Dateiname verwendet wird, der keine verbotenen Zeichen enthält, wird er vor seiner Verwendung entsprechend bereinigt und verbotene Zeichen durch „_“ (Unterstrich) ersetzt. Im

Normalfall wird somit der Dateiname nicht exakt dem SubjectDN entsprechen. Durch eine hinreichende Ähnlichkeit wird eindeutig zu erkennen sein, um welches Zertifikat es sich handelt.

4 Umgang mit Zertifikatssperrlisten (CRLs)

4.1 Zertifikatssperrlisten importieren

Analog zur Verfahrensweise beim Import von Zertifikaten, können auch Zertifikatssperrlisten in die iQ.Suite importiert werden. Der Importvorgang verläuft für beide Plattformen über die Zertifikatssperrlisten-Datenbank. Unter Lotus Notes Domino entspricht das der g_certs.nsf, unter Exchange der Cache-Datenbank. Der Datenbankname ist von der Konfiguration abhängig.

Beim Importieren von Zertifikatssperrlisten bestehen nachfolgende Möglichkeiten:

- **Lokaler CRL-Import**

Bei einem Lokalen CRL-Import werden bereits vorhandene Zertifikatssperrlisten lokal in die iQ.Suite importiert. Die Sperrlisten müssen in einem bestimmten Importordner innerhalb des Dateisystems abgelegt sein, welcher in der Konfiguration angegeben wird. Nach erfolgreichem Import werden die CRLs aus dem Dateisystem gelöscht.
- **Remote CRL-Import**

Bei einem Remote CRL-Import werden Zertifikatssperrlisten, die auf externen Internetseiten zur Verfügung stehen per Remote importiert. Dazu werden zunächst die Zertifikate, die in der Zertifikatsdatenbank der iQ.Suite abgelegt sind analysiert. Sind in den Zertifikaten Informationen (DPIs) enthalten, auf welchen externen Internetseiten CRLs zur Verfügung stehen (komplette Pfadangabe „full name“ erforderlich), kann auf die dort abgelegten Zertifikatssperrlisten per Remote zugegriffen werden. Anschließend werden die Sperrlisten in die Zertifikatssperrlisten-Datenbank per LDAP, LDAPS, LDAPi, FTP oder HTTP importiert (Remote CRL-Import).

Es werden grundsätzlich nur aktuelle CRLs mit der Dateierdung „.crl“ importiert. Abgelaufene Sperrlisten, für die bereits eine neue CRL erschienen sein müsste, werden nicht importiert. Nach dem Importvorgang wird ein Revocation Check durchgeführt, siehe [Revocation Check durchführen](#).

Hinweis: Das Format für zu importierende CRL-Listen muss „DER encoded X.509 (.CRL)“ oder „Base-64 encoded X.509 (.CRL)“ sein.

4.1.1 Beispiel: Zertifikatssperrlisten importieren

Erfahrungsgemäß wird der Zertifikatsmanager so eingesetzt, dass zunächst ein lokaler CRL-Import und anschließend ein Remote CRL-Import erfolgt. Dieser Ablauf ist nachfolgend beschrieben:

1. Stellen Sie sicher, dass alle zu importierenden Zertifikatssperrlisten in dem durch die Konfiguration vorgegebenen Ordner innerhalb des Dateisystems abgelegt sind und die Dateiendung „.crl“ besitzen.
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) angegeben. Um zunächst einen lokalen und anschließend einen Remote CRL-Import durchzuführen, wählen Sie als Parameteraufruf unter **Arbeitsmodus** den Parameter **CRL_IMPORT** aus.
4. Die lokalen CRLs werden in die Zertifikatssperrlisten-Datenbank importiert und aus dem Dateisystem gelöscht (Lokaler CRL-Import).
5. Die in der Zertifikatsdatenbank enthaltenen Zertifikate werden auf bestimmte Informationen innerhalb der DPs geprüft. Werden die erforderlichen Informationen gefunden erfolgt ein Verbindungsaufbau auf die externen Zertifikatssperrlisten und ein anschließender Import in die Zertifikatssperrlisten-Datenbank (Remote CRL-Import).
3. Pro **Arbeitsmodus** wird eine eigene Logdatei geschrieben.
4. Im Anschluss erfolgt ein Revocation Check, siehe [Revocation Check durchführen](#).

Hinweis: Um lediglich einen lokalen CRL-Import durchzuführen, wählen Sie als Parameteraufruf unter **Arbeitsmodus** den Parameter **CRL_IMPORT_LOCAL** auf. Um lediglich einen Remote CRL-Import durchzuführen, wählen Sie als Parameteraufruf unter **Arbeitsmodus** den Parameter **CRL_IMPORT_REMOTE** auf.

4.2 Zertifikatssperrlisten exportieren

Zertifikatssperrlisten, die sich in der Zertifikatssperrlisten-Datenbank befinden, können in das Dateisystem exportiert werden. Hierbei werden die CRLs in einen bestimmten Ordner exportiert, der von der Konfiguration vorgegeben ist.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass alle zu exportierenden Zertifikatssperrlisten in der Zertifikatssperrlisten-Datenbank enthalten sind und die Dateiendung „.crl“ besitzen.
2. Starten Sie den Zertifikatsmanager wie unter [Zertifikatsmanager starten](#) angegeben. Um einen CRL-Export durchzuführen, wählen Sie als Parameteraufruf unter **Arbeitsmodus** den Parameter **CRL_EXPORT** aus.

3. Die Logdatei „iQSuite_crl_export.out“ protokolliert den Sperrlistenexport. Diese wird unter Lotus Notes Domino in das iQSuite DataDir geschrieben, unter Exchange in dem Verzeichnis erzeugt, in dem sich der Zertifikatsmanager befindet.

Hinweis: Der Dateiname der exportierten CRL's setzt sich aus einer verkürzten Form des IssuerDN (Aussteller der CRL) sowie eines eindeutigen Hash Wertes zusammen, um ein Überschreiben bei erneutem Export zu vermeiden.

Der Export der CRL erfolgt in den in der Konfiguration angegebenen Ordner in zwei Formaten:

- als lesbare Datei mit der Endung „...decoded.txt“
- als binäre Datei mit der Endung „...encoded.crl“.

4.3 Zertifikatssperrlisten löschen

Nicht mehr aktuelle Zertifikatssperrlisten werden durch neue ergänzt. Die Information darüber, wann eine neue Zertifikatssperrliste erscheint, ist innerhalb der Zertifikatssperrliste enthalten. Um veraltete Zertifikatssperrlisten aus der Zertifikatssperrlisten-Datenbank zu löschen, wählen Sie als Arbeitsmodus **CRL_REMOVE_OLD** aus. Das Protokoll, welches während des Löschvorgangs geschrieben wurde, wird in der Log-Datei „iQSuite_crl_remove_old.out“ gespeichert.

Hinweis: Verwenden Sie den Modus **CRL_REMOVE_OLD** nur dann, wenn keine S/MIME Jobs aktiviert sind.

5 Revocation Check

Nach Abschluss eines Zertifikatssperrlisten-Imports (Lokal oder per Remote) wird ein Revocation Check durchgeführt. Die Seriennummer sämtlicher Zertifikate, die sich in der Zertifikatsdatenbank der iQ.Suite befinden werden mit den Zertifikatssperrlisten der Zertifikatssperrlisten-Datenbank verglichen. Zertifikate, die in einer CRL aufgelistet sind, werden wie folgt behandelt:

- Unter LND: die Zertifikate erhalten den Vertrauensstatus „not trusted“. Das Feld „Revoked“ wird mit dem Wert „1“ in das Zertifikatsdokument geschrieben.
- Unter Exchange: die Zertifikate werden unmittelbar gelöscht.

Ist das Zertifikat in keiner CRL enthalten, wird der Ausstellerpfad untersucht. Alle Ausstellerzertifikate werden auf die gleiche Weise analysiert und bei Bedarf wie oben beschrieben auf revoked gesetzt bzw. aus der Zertifikatsdatenbank gelöscht. Sobald in einem Zertifikat das Feld „Revoked“ mit dem Wert „1“ gefunden wird, wird die Analyse des Ausstellerpfades abgebrochen.

Hinweis: Beachten Sie, dass weder für den Revocation Check noch für den Umgang mit Zertifikatssperrlisten die „tk_smime“ verwendet wird. Der Zertifikatsmanager arbeitet selbständig. Wurde ein Zertifikat vom Zertifikatsmanager als nicht vertrauenswürdig kategorisiert, so wird dieses Zertifikat bei einer späteren E-Mail-Bearbeitung nicht von „tk_smime“ verwendet.

6 Zertifikatsmanager starten

6.1 Parameterruf

Um den Zertifikatsmanager zu starten, führen Sie die Datei **(n)tk_certmgr.exe** aus. Dies kann über nachfolgende Methoden erfolgen:

- über ein Parameterfile „(n)tk_certmgr.exe @paramfile.txt“ :
Der Name dieser Datei ist beliebig wählbar, es darf jedoch in jeder Zeile lediglich ein Parameter enthalten sein.
- über die Kommandozeile:
„(nt)tk_certmgr.exe <Arbeitsmodus> <Pfadname Zertifikatsdatenbank> <Pfadname CRL-Datenbank> <Arbeitsverzeichnis> <Ausführungsmodus> <Sleeping time> <Logging mode> <LDAP-Server> <LDAP-Port> <LDAP-User> <LDAP-Passwort> <LDAP-Library>“

Geben Sie in beiden Fällen die Parameter in der angegebenen Reihenfolge an und verwenden Sie für Pfadnamen absolute Pfade. Alle Parameter müssen konfiguriert werden. Beachten Sie insbesondere den Parameter **<Arbeitsmodus>**, da dieser die eigentliche Aktion des Zertifikatsmanagers festlegt, z.B. Zertifikate importieren, oder Zertifikatssperrlisten exportieren.

6.2 Modi des Parameterrufs

Nachfolgende Parameter stehen Ihnen beim Parameterruf des Zertifikatsmanagers zur Verfügung. Alle Parameter müssen konfiguriert werden.

- **<Arbeitsmodus>**:
 - **IMPORT**: Import der Zertifikate
 - **EXPORT**: Export der Zertifikate
 - **CRL_IMPORT_LOCAL**: Lokaler Import der CRL-Listen aus dem Dateisystem. Die lokalen CRLs, die sich im CRL-Import-Ordner befinden, werden importiert.

Anschließend werden die CRL aus dem Dateisystem gelöscht. Beachten Sie, dass nur aktuelle CRLs berücksichtigt werden.

- **CRL_IMPORT_REMOTE:** Import der CRL-Listen (remote).
Die CRL werden per LDAP, FTP oder HTTP importiert. Das passiert nur, wenn die Zertifikate, die sich in der Zertifikatsdatenbank befinden, die entsprechenden Distribution Point Informationen enthalten, d.h. wo CRL remote geladen werden können. Hier erfolgt ebenfalls nur der Import von aktuellen CRL. Hierfür müssen die entsprechenden Standardports (LDAP, FTP, http) an der Firewall freigegeben sein.
- **CRL_IMPORT:** Import der CRL-Listen (Lokaler und Remote CRL-Import).
Die CRL-Listen werden erst entsprechend dem Arbeitsmodus **CRL_IMPORT_LOCAL** und anschließend entsprechend **CRL_IMPORT_REMOTE** importiert.
- **CRL_EXPORT:** Export der CRL-Listen
- **CRL_REMOVE_OLD:** Löschen alter CRLs aus der Zertifikatssperrlisten-Datenbank. Beachten Sie unter LND, dass keine S/MIME-Jobs aktiviert sein dürfen. Anderenfalls muss der MailGrabber gestoppt und nach dem Lauf des Zertifikatsmanagers wieder gestartet werden.

■ **<Pfadname Zertifikatsdatenbank>:**

Tragen Sie den Pfadnamen der verwendeten Zertifikatsdatenbank ein. Der Pfadname setzt sich aus dem kompletten Pfad sowie dem Namen der verwendeten Datenbank zusammen.

- Bei LND: Der Name der Zertifikatsdatenbank muss ohne Endung angegeben werden, z.B.: C:\Lotus\Data\iQSuiteData\g_cert
- Bei Exchange: Der Name der Zertifikatsdatenbank kann beliebig gewählt werden, z.B.: ... \certs.db

■ **<Pfadname CRL-Datenbank>:**

Tragen Sie den Pfadnamen der verwendeten Zertifikatssperrlisten-Datenbank ein. Der Pfadname setzt sich aus dem kompletten Pfad sowie dem Namen der verwendeten Datenbank zusammen.

- Bei LND: Der Name der Zertifikatssperrlistendatenbank muss ohne Endung angegeben werden, z.B.: C:\Lotus\Data\iQSuiteData\g_cert
- Bei Exchange: Der Name der Zertifikatssperrlistendatenbank (Cache-Datenbank) kann beliebig gewählt werden, z.B.: ... \certs.db

■ **<Arbeitsverzeichnis>:**

Geben Sie den kompletten Pfad zu dem Verzeichnis an, welches die für den Import bzw. Export benötigten Unterordner und Zertifikate enthält, z.B.:

```
C:\Domino\iQSuite\smime\Import oder
C:\Domino\iQSuite\smime\Export oder
C:\Domino\iQSuite\smime\crl_import oder
C:\Domino\iQSuite\smime\crl_export.
```

■ **<Ausführungsmodus>:**

Um die Zertifikate bzw. Zertifikatssperrlisten je nach Konfiguration der Parameter importieren oder exportieren zu können, geben Sie den gewünschten Ausführungsmodus an:

- CMDLINE: Die **exe-Datei** wird über die Kommandozeile einmalig ausgeführt.
- Nur bei LND: SRVTASK: Die **exe-Datei** wird als Server-Add-In einmalig ausgeführt.

■ **<Sleeping time>:**

Zeitraum, der zwischen den einzelnen Durchläufen gewartet wird (Angabe in Sek.).

■ **<Logging mode>:**

- NORMAL
Standard-Logausgabe des Zertifikatsmanagers. Das Logging erfolgt auf der Serverkonsole.
- SILENT
Reduzierte Logausgabe. Lediglich der Start- und Endezeitpunkt des Zertifikatsmanagers wird geloggt.

■ **<LDAP-Server>:**

Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, von dem die CRL-Listen importiert werden. Soll dieser Parameter nicht verwendet werden, tragen Sie den Wert „0“ ein.

■ **<LDAP-Port>:**

Geben Sie den Port an, auf dem der LDAP-Server für den Import der CRL-Listen angesprochen werden soll. Soll dieser Parameter nicht verwendet werden, tragen Sie den Wert „0“ ein.

■ **<LDAP-User>:**

Tragen Sie den Namen des LDAP-Users ein, mit dem der LDAP-Server für den Import der CRL-Listen angesprochen werden soll. Soll dieser Parameter nicht verwendet werden, tragen Sie den Wert „0“ ein.

■ **<LDAP-Passwort>:**

Geben Sie das Passwort des LDAP-Users an, mit dem der LDAP-Server für den Import der CRL-Listen angesprochen werden soll. Soll dieser Parameter nicht verwendet werden, tragen Sie den Wert „0“ ein.

■ **<LDAP-Library>:**

Tragen Sie eine alternative LDAP-Library bzw. DLL ein, mit deren Hilfe der LDAP-Zugriff erfolgen soll. Soll dieser Parameter nicht verwendet werden, tragen Sie den Wert „0“ ein.

© 2008 GROUP Technologies AG

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der GROUP Technologies AG zum Zeitpunkt der Veröffentlichung dar. Da GROUP Technologies AG auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens der GROUP Technologies AG dar und GROUP kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient nur zu Informationszwecken. Die GROUP Technologies AG schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck.

Alle in diesem Dokument aufgeführten Produkt- oder Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.



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>