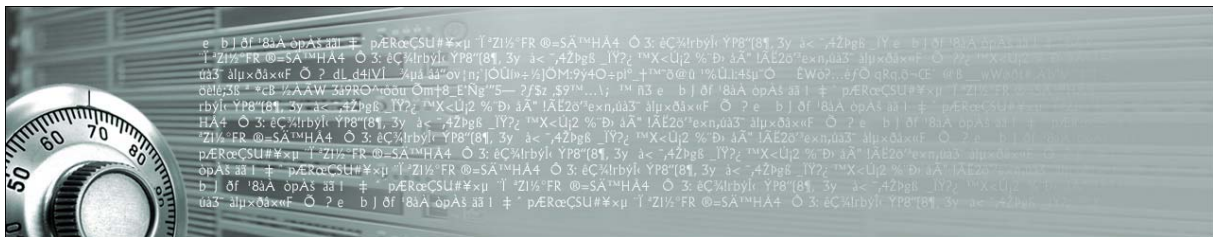

CERTUS ♦ LATEO

Realtime communication encryption layer system

Benutzerhandbuch

Programm - Version 4.8.9

Manual Release 091126



Copyright © 2009 by Barclay Technologies (Schweiz) AG. Alle Rechte vorbehalten.

Inhaltsverzeichnis

| | | |
|----|---|----|
| 1. | Einleitung..... | 5 |
| | Prolog..... | 5 |
| | Was ist Certus Lateo™ ? | 5 |
| | Einleitung..... | 5 |
| | Funktionsweise | 5 |
| | Verschlüsselungsprinzip..... | 6 |
| | Performance und Sicherheit..... | 6 |
| | Funktionsumfang | 6 |
| | Die Komponenten von Certus Lateo™ | 7 |
| 2. | Installation | 8 |
| | Vorbereitung..... | 8 |
| | Updater | 8 |
| | Lokale Installation Certus Lateo™..... | 8 |
| | Lokale Installation über die CMD Konsole (Eingabeaufforderung)..... | 9 |
| | Installation der Certus Lateo™ MMC Admin Console | 9 |
| | Installation Certus Lateo™ Admin Panel | 9 |
| | Netzwerkinstallation | 10 |
| | Installation von Updates | 10 |
| 3. | Certus Lateo™ MMC Admin Console..... | 11 |
| | Starten der MMC Admin Console | 11 |
| | Die Bereiche der MMC Admin Console | 11 |
| | Root..... | 11 |
| | Übersicht..... | 11 |
| | Aktionen | 12 |
| | Funktionen | 12 |
| | Add Group (Erstellen neuer Gruppen)..... | 12 |
| | Refresh Groups (Gruppenliste Aktualisieren) | 12 |
| | Refresh Computers (Computerliste Aktualisieren) | 12 |
| | Show License Information (Lizenzinformationen anzeigen) | 12 |
| | Refresh License Information (Lizenz Aktualisieren) | 12 |
| | Rename (Ändern einer Gruppenbezeichnung)..... | 12 |
| | Move (Rechner einer Gruppe zuweisen) | 12 |
| | Delete (Rechner löschen)..... | 13 |
| | Edit (Konfigurieren einer Gruppe) | 13 |
| 4. | Certus Lateo™ Admin Panel..... | 15 |
| | Start..... | 15 |
| | Konfigurationen..... | 15 |
| | Protokoll..... | 16 |
| | Liste..... | 16 |
| | Config | 16 |
| | IP und Port Settings | 17 |
| 5. | Anhang..... | 18 |
| | Systemvoraussetzungen | 18 |
| | Weitere Voraussetzungen..... | 18 |
| | Anhang A: Enduser Lizenzvereinbarung | 19 |

1. EINLEITUNG

PROLOG

Immer wieder wird bekannt, dass vertrauliche oder sensible Daten von Unternehmen und Behörden gestohlen werden oder ungewollt an die Öffentlichkeit gelangen, was sehr schnell zu einem Image- oder gar wirtschaftlichen Schaden führen kann. Dabei sind Angriffe durch fremde Hacker ein weit geringeres Problem als Fehler, Fahrlässigkeit oder gar kriminelles Verhalten der eigenen Mitarbeiter.

Dies überrascht kaum, wenn man bedenkt, wie viele Personen jeweils Zugriff auf die entsprechenden Daten haben müssen um ihrer täglichen Arbeit nachgehen zu können.

Schnell wird ein Datenträger irgendwo liegengelassen oder Dateien kurzerhand auf einen Massendatenspeicher (z.B. USB Stick / CD / DVD) kopiert und an Unbefugte weitergegeben.

Für Unternehmen sind verschiedenste Daten von grossem Wert, seien es Kundendaten, Projektbezogene Unterlagen, Strategiepläne oder Software Sourcen. Sie bilden nicht selten das eigentliche Kapital einer Firma. Solche Daten vor dem Zugriff durch Unberechtigte zu schützen, stellt in der heutigen Zeit eine der grössten innerbetrieblichen Herausforderungen dar.

Eine der besten Möglichkeiten um Daten zu schützen sind Verschlüsselungs- sowie DLP (Data Loss Prevention) Systeme. In der Regel bringen diese jedoch eine komplizierte Handhabung, grossen Zeitaufwand sowie eine Flut von Passwörtern mit sich, welche selbst wiederum sicher verwahrt werden müssen. Mit den verschlüsselten Daten kann zudem nicht direkt gearbeitet werden, weshalb die Daten jeweils immer entschlüsselt werden müssen, wonach wieder sämtliche Möglichkeiten offen stehen, Daten für unerlaubte Aktivitäten zu verwenden.

Solche Überwachungs-Software ist zwar hilfreich, um herauszufinden wer worauf zugegriffen hat, jedoch verhindert sie keinen Datendiebstahl. Sie kann nur schlecht zwischen einem autorisierten Zugriff und einem unautorisierten Zugriff für das möglicherweise unerlaubte Erstellen einer Kopie unterscheiden.

Doch auch wer sich voll auf seine Mitarbeiter verlassen kann ist vor Datendiebstahl nicht sicher. Es ist für Profis und Hacker heute nach wie vor möglich in Unternehmensnetze einzudringen oder diese abzu hören oder zu infiltrieren und sich so Zugang zu vertraulichen Daten zu beschaffen.

Mit Certus Lateo™ wurde nun ein System entwickelt, welches äusserst sicher, effizient und vom Benutzer praktisch unbemerkt sowohl ungewollte als auch mutwillige Verbreitung von Daten, wie auch das Abfangen von übertragenen Daten zuverlässig verhindert.

WAS IST CERTUS LATEO™ ?

EINLEITUNG

Certus Lateo™ schützt sensible Daten von Unternehmen und Behörden und Organisationen effizient vor dem Zugriff durch Unberechtigte, ohne dabei den gewohnten Arbeitsablauf zu erschweren.

Dies wird durch die komplette Abriegelung eines Computers erreicht, welcher nur mit Systemen kommunizieren kann, welche ebenfalls über Certus Lateo™ mit der gleichen Berechtigung verfügen.

FUNKTIONSWEISE

Ein Nutzer der Certus Lateo™ Technologie, verfügt über eine für seine Umgebung lizenzierte Installation, wodurch nur die von ihm vorgesehenen Geräte mit installiertem Certus Lateo™ Zugriff auf die verschlüsselten Daten erhalten.

Certus Lateo™ wird als Treiber dezent im Hintergrund des Betriebssystems ausgeführt und ver- und entschlüsselt sämtliche ein- und ausgehenden Daten des gesamten Systems.

Für den Benutzer entfallen dadurch umständliche manuelle Ver- und Entschlüsselungsvorgänge mittels einer separaten Software.

VERSCHLÜSSELUNGSPRINZIP

Certus Lateo™ verwendet eine eigene völlig neue, äusserst innovative und hochsichere Verschlüsselungstechnologie.

Beim Versenden von Daten über eine Netzwerkverbindung wird für jedes Datenpaket ein völlig neuer Schlüssel in gleicher Grösse wie das Datenpaket selbst, mittels variablen, dynamischen Algorithmen generiert und angewendet.

Der Schlüssel selbst muss dabei nicht mitübertragen werden. Stattdessen werden der Gegenseite mittels dynamisch eingebeteter Indizien die notwendigen Informationen übermittelt, welche zur Reproduktion des richtigen Algorithmus zur Entschlüsselung des Datenpakets notwendig sind.

Durch die einmalige Verwendung eines Schlüssels in gleicher Länge, wie die zu verschlüsselnden Daten selbst, entsteht eine mathematisch nicht rekonstruierbare und somit absolut sichere Verschlüsselung.

Ein weiterer Vorteil dieses Verfahrens zeigt sich auch durch die geringe Rechenleistung, welche für die Verschlüsselung benötigt wird, da die zu verarbeitenden Datenmengen im Vergleich zur Verschlüsselung ganzen Dateien äusserst klein sind und in Echtzeit vorgenommen werden können.

PERFORMANCE UND SICHERHEIT

Gegenüberstellung führenden Technologien (Twofish, AES, Caesar) und Certus Lateo™

| | Standard | CL |
|---|-------------------|----------------|
| Schlüssellänge | 128, 192 oder 256 | 1024 und höher |
| Performance (Verschlüsselte Zeichen pro ms) (Standard Workstation) | 20'000 | 80'000 |
| Benötigte Rechenzeit zum knacken. (Optimierte Workstation) | ab wenigen tagen | nicht möglich |
| Algorithmus | öffentlich | variabel |
| Markteinführung | ab 1998 | 2009 |

FUNKTIONSUMFANG

Verschlüsselungs- und Sperrfunktionen:

- Netzwerkverbindungen (Ethernet)
- Firewire (IEEE 1394)
- USB Geräte
- CD / DVD Laufwerke (Sperrern)
- Bluetooth
- Speichersticks
- Externe Festplatten
- Speicherkarten
- RS232

DIE KOMPONENTEN VON CERTUS LATEO™

Certus Lateo™ besteht zum einen aus der System Software, welche die Treiber und Dienste beinhaltet und auf jedem Computer installiert wird, sowie dem separaten Administrations Panel zur Konfiguration der Geräte für den Systemadministrator.

CERTUS LATEO™

Certus Lateo™ verschlüsselt die Netzwerkverbindungen eines Systems. Dadurch wird es für Unbefugte unmöglich, Zugriff über eine Netzwerkverbindung herzustellen oder gar Daten abzufangen und zu lesen. Vielmehr ist ein mit Certus Lateo™ gesichertes System/Netzwerk für aussenstehende Geräte gar nicht erkennbar, da auch die zur Identifikation notwendige Kommunikation verschlüsselt stattfindet.

Certus Lateo™ schützt sowohl Ethernet als auch Firewire Netzwerkverbindungen.

Certus Lateo™ sperrt oder verschlüsselt zudem die Kommunikation mit Peripheriegeräten. Dadurch wird es unmöglich, Daten ausserhalb der berechtigten Umgebung zu nutzen, da diese beim Verlassen des Systems direkt verschlüsselt werden.

Werden beispielsweise Daten auf einen Massendatenspeicher wie USB Memorystick kopiert, werden diese automatisch verschlüsselt. Auf einem System ohne Certus Lateo™ sind diese danach nicht mehr lesbar. Erst beim Zugriff durch ein berechtigtes Gerät werden die vorhanden Daten umgehend wieder entschlüsselt und können ohne weitere Aktionen verwendet werden.

Certus Lateo™ schützt, USB Ports, CD / DVD Laufwerke, Bluetooth-Verbindungen, Speichersticks, RS 232 Schnittstellen sowie andere externe Datenspeicher wie Festplatten oder Speicherkarten.

2. INSTALLATION

Bei der Installation der Certus Lateo™ Komponenten ist zu beachten, dass diese mit Administrator-Rechten durchgeführt werden muss und einen Neustart des Systems erforderlich ist.

Nach der Installation bzw. dem Neustart, ist das System noch Ungeschützt und kann unverändert genutzt werden, bis die gewünschten Konfigurationen durch den Certus Lateo™ Administrator mittels des Certus Lateo™ MMC Console oder Admin Panels vorgenommen wurden.

Dies ermöglicht eine koordinierte Umstellung aller Computer zu einem bestimmten, gemeinsamen Zeitpunkt.

VORBEREITUNG

Bevor Certus Lateo™ installiert und aktiviert wird, sollten einige Punkte beachtet werden:

- Benutzer des Systems dürfen nicht über Administrationsrechte verfügen. Als Administrator hat ein Benutzer weitreichende Berechtigungen auf Systemebene die Möglicherweise genutzt werden können um Funktionen von Certus Lateo™ zu manipulieren.
- Notieren Sie sich im Vorfeld, wie Sie Ihr System konfigurieren wollen. Welche Rechner/Arbeitsplätze über welche Rechte verfügen und über welche Ports und IP Adressen allenfalls unverschlüsselt kommuniziert werden soll oder muss (Z. Bsp. Netzwerkdrucker, Datenbankserver etc.).
- Stellen Sie sicher, dass Sie allenfalls ergänzende Sicherheitsvorkehrungen zum Schutz Ihrer Daten getroffen haben die nicht durch Certus Lateo™ gedeckt werden können. (Z. Bsp. Hardware Diebstahl etc.)

UPDATER

Certus Lateo™ wird kontinuierlich weiterentwickelt. Die neuesten Versionen können über den Certus Lateo Updater heruntergeladen werden.

Diese Updates dienen der Verbesserten Handhabung, Leistungsoptimierung, Anpassungen an neue Systeme und Betriebsumgebungen usw.

Nach dem Download werden die bestehenden Setup-Dateien auf dem USB Dongle automatisch durch die neueren Versionen ersetzt.

LOKALE INSTALLATION CERTUS LATEO™

Certus Lateo™ wird über das reguläre Setup installiert.

Es benötigt keine Benutzereingaben.

Die jeweiligen Treiberdateien werden automatisch installiert und die notwendigen Registrationen vorgenommen.

Nach der Installation ist ein Neustart des Systems erforderlich.

Wichtig:

Unter Windows Vista sowie Windows 7 muss das Setup zwingend als „Administrator“ ausgeführt werden.

Um .msi Pakete unter diesen Betriebssystemen als Administrator installieren zu können, muss gegebenenfalls der Umweg über die CMD Konsole genommen werden.

LOKALE INSTALLATION ÜBER DIE CMD KONSOLE (EINGABEAUFFORDERUNG)

Für die lokale Installation ab Windows Vista (dementsprechend auch unter Windows 7), muss das .msi Setup als "Administrator" ausgeführt werden, um die benötigten Rechte zur Treiberinstallation zu erhalten. Diese können im Gegensatz zu .exe Dateien jedoch nicht direkt als "Administrator" gestartet werden, sondern müssen über die CMD Konsole (Eingabeaufforderung) aufgerufen werden.

1. Öffnen Sie im Windows Startmenü unter Programme/Zubehör die CMD Konsole, indem Sie mit einem Rechtsklick auf die "Eingabeaufforderung" den Menüpunkt "Als Administrator ausführen" auswählen.

2. Wechseln Sie nun auf das Laufwerk auf welchem sich das Certus Lateo™ .msi Setup befindet. (Eingabe des Laufwerksbuchstaben mit "Doppelpunkt" und anschließender Bestätigung durch "Enter".
Z.Bsp. *F: [enter]*)

3. Öffnen Sie sofern erforderlich den Ordner, in welchem sich die benötigte Setup Datei befindet.
(Z. Bsp: *cd programme/certuslateo/setup [enter]*)

4. Starten Sie nun das Setup indem Sie den entsprechenden Dateinamen eingeben und mit "Enter" bestätigen.

(Z. Bsp. *setup.msi [enter]*)

Die Rechte der CMD Konsole gelten nun auch für die Ausführung der .msi Installationsdatei.

TIPP: Nach der Eingabe der Anfangsbuchstaben erhalten Sie mit der Tabulator-Taste (Tab) nacheinander die im jeweiligen Verzeichnis verfügbaren Dateien angezeigt.

Nach der Installation ist ein Neustart des Systems erforderlich.

INSTALLATION DER CERTUS LATEO™ MMC ADMIN CONSOLE

Vor der Installation des Certus Lateo™ Admin Panels muss auf dem jeweiligen Rechner bereits Certus Lateo™ installiert sein.

1. Starten Sie für die Installation die Setup Datei mit den erforderlichen Rechten und folgen Sie den Anweisungen.

Das Setup erstellt im Windows® Startmenu sowie auf dem Desktop eine Verknüpfung zum „Certus MMC Admin“ über welche die Administrations-Applikation geöffnet wird.

Die Certus Lateo™ MMC Admin Console kann auch als Snap-In in die Windows Microsoft Management Console geladen werden.

INSTALLATION CERTUS LATEO™ ADMIN PANEL

Vor der Installation des Certus Lateo™ Admin Panels sollte auf dem jeweiligen Rechner bereits Certus Lateo™ installiert sein.

1. Starten Sie für die Installation die Setup Datei und folgen Sie den Anweisungen.
2. Während der Installation werden Sie aufgefordert ein Administrator Passwort zu definieren. Dieses wird später zum öffnen des Admin Panel benötigt um unberechtigtes Ändern der Konfigurationen zu verhindern.

Nach der Installation ist ein Neustart des Systems erforderlich.

Für den korrekten Betrieb des Admin Panels muss die Applikation gegebenenfalls noch bei einer lokalen Firewall freigeschaltet werden.

NETZWERKINSTALLATION

Die Certus Lateo™ .msi Setup Dateien können mit den gängigen Systemen auch über ein Netzwerk verteilt und installiert werden.

Achten Sie darauf das alle erforderlichen Berechtigungen für die Verteilung sowie die Installation von Treibern verfügen.

INSTALLATION VON UPDATES

Um Certus Lateo™ zu aktualisieren muss lediglich die neueste Version über die bestehende installiert werden.

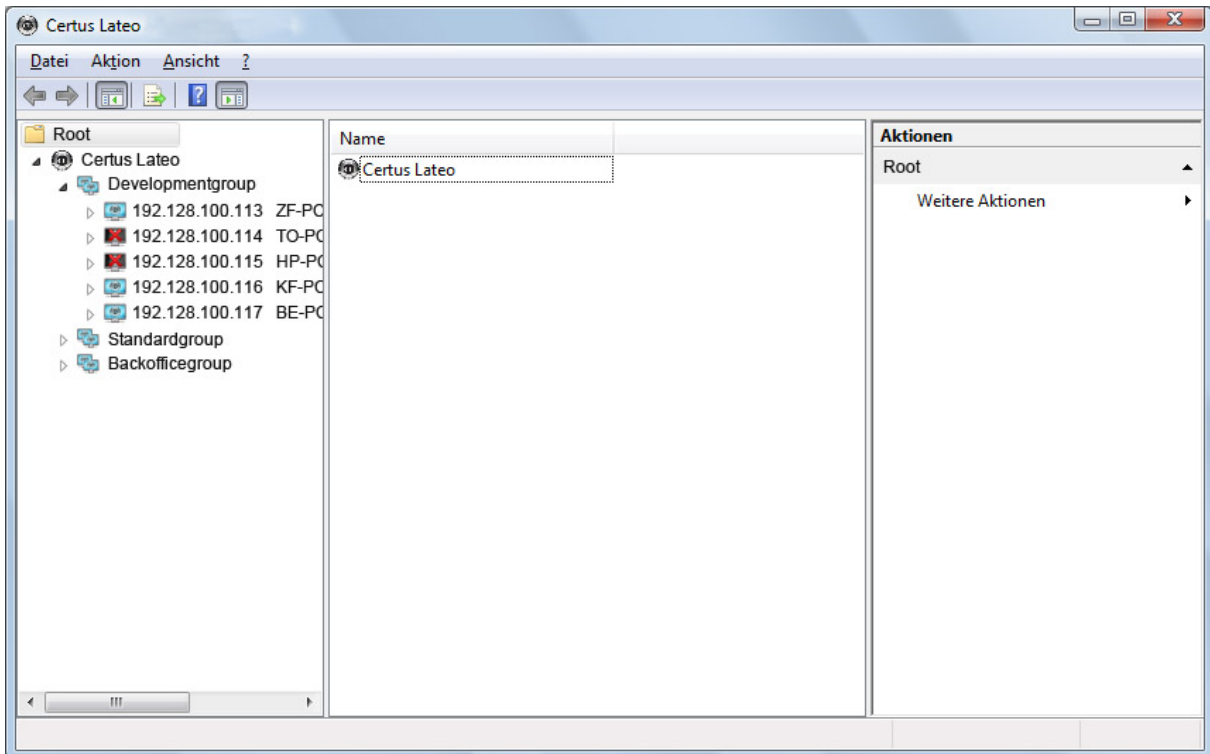
Sobald eine neue Version Verfügbar ist, kann diese mit der "Certus Lateo Updater" Applikation auf dem USB Dongle heruntergeladen werden. Nach dem Download wird die veraltete Setup-Datei auf dem USB Stick automatisch überschrieben.

Die Updates müssen für jeden USB Dongle separat heruntergeladen werden.

Die Installation der jeweiligen Komponenten wird wie oben beschrieben durchgeführt. Im Verlauf der Installation wird allenfalls die Meldung "Files in Use" angezeigt, welche jedoch einfach übersprungen werden kann.

3. CERTUS LATEO™ MMC ADMIN CONSOLE

Mit der MMC Admin Console verwaltet der Certus Lateo™ Administrator die Konfigurationen des Systems. Dabei werden Gruppen mit den gewünschten Einstellungen erstellt und die dem Certus Lateo™ Netzwerk angehörenden Geräte der jeweiligen Gruppe zugeordnet.



STARTEN DER MMC ADMIN CONSOLE

Die MMC Admin Console kann über die Verknüpfung unter START/Programme/Barclay Technologies gestartet werden.

Im Anschluss werden Sie aufgefordert, Ihren Certus Lateo™ USB Dongle einzustecken. Dieser wird mit dem Certus Lateo™ Setup ausgeliefert und dient zur eindeutigen Identifikation des berechtigten Administrators.

Bewahren Sie diesen also an einem gut geschützten Ort auf.

DIE BEREICHE DER MMC ADMIN CONSOLE

ROOT

Im Root im linken Fenster der MMC Admin Console werden unter „Certus Lateo“ die eingerichteten Gruppen angezeigt.

Die "DefaultGroup" ist vom System vorgegeben und kann weder gelöscht noch umbenannt werden. Hier drin werden sämtliche Rechner aufgeführt, welche noch keiner Gruppe zugewiesen wurden.

ÜBERSICHT

Im mittleren Bereich der MMC Admin Console werden detailliertere Informationen zu dem im Root angewählten Eintrag angezeigt. Es werden die verfügbaren Gruppen bzw. bei der Selektion einer bestimmten Gruppe die darin enthaltenen Rechner aufgelistet.

Links neben den aufgelisteten Rechnern zeigt das Icon den Verbindungsstatus des jeweiligen Gerätes an.



Gerät ist online



Gerät ist offline

AKTIONEN

Im rechten Bereich der MMC Amin Console finden Sie die Spalte „Aktionen“ in welcher die verfügbaren Funktionen aufgelistet werden. Diese sind abhängig von dem jeweils in der Übersicht selektierten Eintrag.

FUNKTIONEN

ADD GROUP (ERSTELLEN NEUER GRUPPEN)

Zum Erstellen einer neuen Gruppe wählen Sie im Root den Eintrag „Certus Lateo“ aus.

Klicken Sie im Bereich „Aktionen“ auf „Add Group“ und geben Sie im Eingabefeld einen beliebigen Namen für die neue Gruppe an.

REFRESH GROUPS (GRUPPENLISTE AKTUALISIEREN)

Diese Funktion aktualisiert die verfügbaren Gruppen, sowie deren zugehörigen Rechner.

REFRESH COMPUTERS (COMPUTERLISTE AKTUALISIEREN)

Wenn neue Rechner im Netz gestartet wurden oder Gruppenzuweisungen geändert wurden kann es erforderlich sein, die Auflistung der Rechner zu aktualisieren.

Es werden dabei sämtliche Rechner in allen Gruppen aktualisiert.

SHOW LICENSE INFORMATION (LIZENZINFORMATIONEN ANZEIGEN)

Über diese Funktion wird ein Fenster mit den aktuellen Lizenzinformationen angezeigt. Diese beinhaltet die Lizenz ID, die verwendete sowie die maximal mögliche Anzahl Rechner und das Ablaufdatum der Lizenz.

REFRESH LICENSE INFORMATION (LIZENZ AKTUALISIEREN)

Wenn die Lizenz durch Ihren Händler erweitert oder verlängert wurde muss sie mit diesem Befehl von Ihrem System aktualisiert werden.

RENAME (ÄNDERN EINER GRUPPENBEZEICHNUNG)

1. Wählen Sie zum Ändern einer Gruppenbezeichnung im Root den Eintrag „Certus Lateo“ aus. Im Übersichtsfenster werden nun sämtliche verfügbaren Gruppen aufgelistet.
2. Klicken Sie auf die Gruppe die Sie umbenennen möchten.
3. Nun finden Sie unter „Aktionen“ den Befehl „Rename“, welcher Ihnen das Ändern der jeweiligen Gruppenbezeichnung erlaubt.

MOVE (RECHNER EINER GRUPPE ZUWEISEN)

1. Öffnen Sie im Verzeichnisbaum die Gruppe in welcher sich der Rechner den Sie zuweisen wollen derzeit befindet.
2. Wählen Sie das gewünschte Gerät aus und klicken Sie im Bereich „Aktionen“ auf die Funktion „Move“.

3. Wählen Sie aus den nun aufgeführten Gruppen die gewünschte aus und bestätigen Sie diese mit „Accept“.

Der jeweilige Rechner ist nun der neuen Gruppe zugewiesen und übernimmt die entsprechenden Einstellungen automatisch.

DELETE (RECHNER LÖSCHEN)

Wenn ein Rechner aus dem System entfernt werden soll, kann er mit dem Befehl "Delete" gelöscht werden. Er wird dabei lediglich aus der Darstellung entfernt und die Lizenz für einen anderen Rechner freigegeben.

EDIT (KONFIGURIEREN EINER GRUPPE)

Wählen Sie im Root und Certus Lateo oder im Übersichtsfenster die gewünschte Gruppe aus. Öffnen Sie anschliessend das Konfigurationsfenster über die Schaltfläche „Edit“ im Bereich „Aktionen“.

Das Fenster für die Gruppenkonfiguration:

- Grundeinstellungen
- Port und IP Eingabefelder
- Übersichtsfenster für bestehenden Port und IP einträge

MASS STORAGE DEVICES

Hier werden die Einstellungen für Massendatenspeicher wie USB Sticks und Speicherkarten vorgenommen.

Open:

Massendatenspeicher können uneingeschränkt verwendet werden.

Locked:

Massendatenspeicher werden gesperrt.

Crypted:

Daten können ausschliesslich in verschlüsselter Form in den dafür vorgesehenen Ordner auf dem Massendatenspeicher geschrieben werden.

WICHTIGE ANMERKUNGEN

Bitte beachten Sie, dass Änderungen für USB Massenspeicher nicht übernommen werden können solange ein Gerät aktiv, also eingesteckt ist und verwendet wird.

Um Verschlüsselte Dateien (Data at rest) wieder zu lesen benötigen Sie einen Rechner mit der gültigen, bei Speicherung verwendeten Lizenz von Certus Lateo™ !

Zusätzliche (sekundäre) interne SATA Disks müssen im BIOS als „erweiterte System-Disk“ konfiguriert sein (enhanced system disc). Andernfalls werden diese vom Betriebssystem unter Umständen als Massendatenspeicher behandelt.

COMPACT DISC'S

Die Berechtigung für das Verwenden von CD und DVD Brennern wird hier verwaltet.

Open:

Die Laufwerke können ohne Einschränkung verwendet werden.

Locked:

Das Schreiben auf CD und DVD Laufwerke wird durch das Deaktivieren der Windows eigenen Schreibfunktion gesperrt.

Die Änderung der Schreibrechte von CD und DVD Laufwerken wird erst nach einem Neustart des Systems übernommen.

WICHTIG:

Soll das Schreiben auf CD und DVD Laufwerke zuverlässig unterbunden werden dürfen keine anderen Applikationen zum Brennen von CDs und DVDs installiert sein, da diese meist direkt aus der jeweiligen Applikation heraus eigene Treiber zum Schreiben verwenden.

NETWORK

Unter Network wird die Verschlüsselung der gesamten Netzwerkkommunikation aktiviert.

Open:

Die Netzwerkverschlüsselung ist deaktiviert.

Crypted:

Die Netzwerkverschlüsselung ist aktiviert. Das System kann nur mit anderen, dem gleichen Certus Lateo™ Netz angehörenden Rechnern verschlüsselt, sowie über die explizit freigegebenen Ports und IP Adressen unverschlüsselt kommunizieren.

SHOW STARTUP SPLASHSCREEN

Der Startup Splashscreen wird beim Starten des Betriebssystems angezeigt und informiert den Benutzer über die installierte Certus Lateo™ Software.

Dieses Info-Fenster kann mittels „true“ angezeigt oder durch Auswählen der Einstellung „false“ deaktiviert werden.

SHOW TRAYICON

Das Trayicon befindet sich bei der Einstellung „true“ rechts in der Taskbar und informiert den Benutzer über die installierte Certus Lateo™ Software. Diese Anzeige kann wie auch der Splashscreen mittels „false“ deaktiviert werden.

PORT UND IP DEFINITIONEN

Grundsätzlich verschlüsselt Certus Lateo™ die gesamte Kommunikation eines Netzwerkes. Es ist jedoch in machen Fällen erforderlich über bestimmte Ports und IP Adressen oder Adressbereiche weiterhin unverschlüsselt zu kommunizieren, da die Gegenseite nicht über die sonst erforderliche Certus Lateo™ Installation verfügt. (Z. Bsp. Netzwerk-Drucker, externe Systeme, alternative Betriebssysteme usw.)

Zu diesem Zweck können sowohl einzelne Ports, Port Bereiche, einzelne IP Adressen sowie IP Adressbereiche definiert werden, über welche in beiden Richtungen unverschlüsselt kommuniziert wird.

Bearbeiten von Port und IP Definitionen:

Um neue Einträge hinzuzufügen werden die entsprechenden Werte in die jeweiligen Felder eingetragen und mit der Schaltfläche „Add“ der Liste hinzugefügt.

Durch selektieren eines Eintrages in der Liste und anschliessendes Drücken von „Delete Selected“ wird der gewählte Eintrag gelöscht.

Die Einstellungen werden schliesslich mit der Schaltfläche „Accept“ übernommen.

Rechner die zum Zeitpunkt der Konfigurationsänderung nicht mit dem System verbunden sind, holen sich die aktuellen Einstellungen automatisch beim nächsten Zugriff auf das Certus Lateo™ Netz.

INTERNET UND EMAIL

An vielen Arbeitsplätzen ist das Internet (Port 80) oft ein unentbehrliches Hilfsmittel für die tägliche Arbeit. Wird dieser Port geöffnet, muss Ihnen jedoch bewusst sein, dass dies eine offene Tür in Ihrem Netz darstellt, über welche beliebige Daten übermittelt werden können. (Beispielsweise über ein Upload Script).

Gleiches gilt beim E-Mail Verkehr. Auch hier können Daten an eine beliebige Partei gesendet werden.

Denken Sie in diesem Fall daran, solche Aktivitäten mit der entsprechenden Infrastruktur zu protokollieren um gegebenenfalls nachvollziehen zu können, wer, was, wann, wohin übermittelt hat und stellen Sie allenfalls sicher, dass den Anwendern bewusst ist, dass diese Aktivitäten nachvollzogen werden können.

4. CERTUS LATEO™ ADMIN PANEL

Das Admin Panel ist ein Administrations Tool welches vor allem bei kleineren Netzwerken zum Einsatz kommt. Im Gegensatz zur MMC Admin Console verfügt es über keine Funktion für die Gruppierung von Rechnern sondern verwaltet diese als eigenständige, individuelle Geräte. Das Admin Panel kann dazu auf jedem dem Certus Lateo™ Umgebung zugehörigen System installiert und genutzt werden.

START

Die Konfiguration der Certus Lateo™ Umgebung, welche durch das Admin Panel bewerkstelligt wird, bedarf eines besonders guten Zugriffsschutzes.

Sowohl das richtige Administrator-Passwort sowie eine Hard- und Software Identifikation (Dongle) wird zum Starten der Applikation benötigt. Dieser Dongle kann nicht kopiert werden und identifiziert den Besitzer somit als berechtigten Administrator.

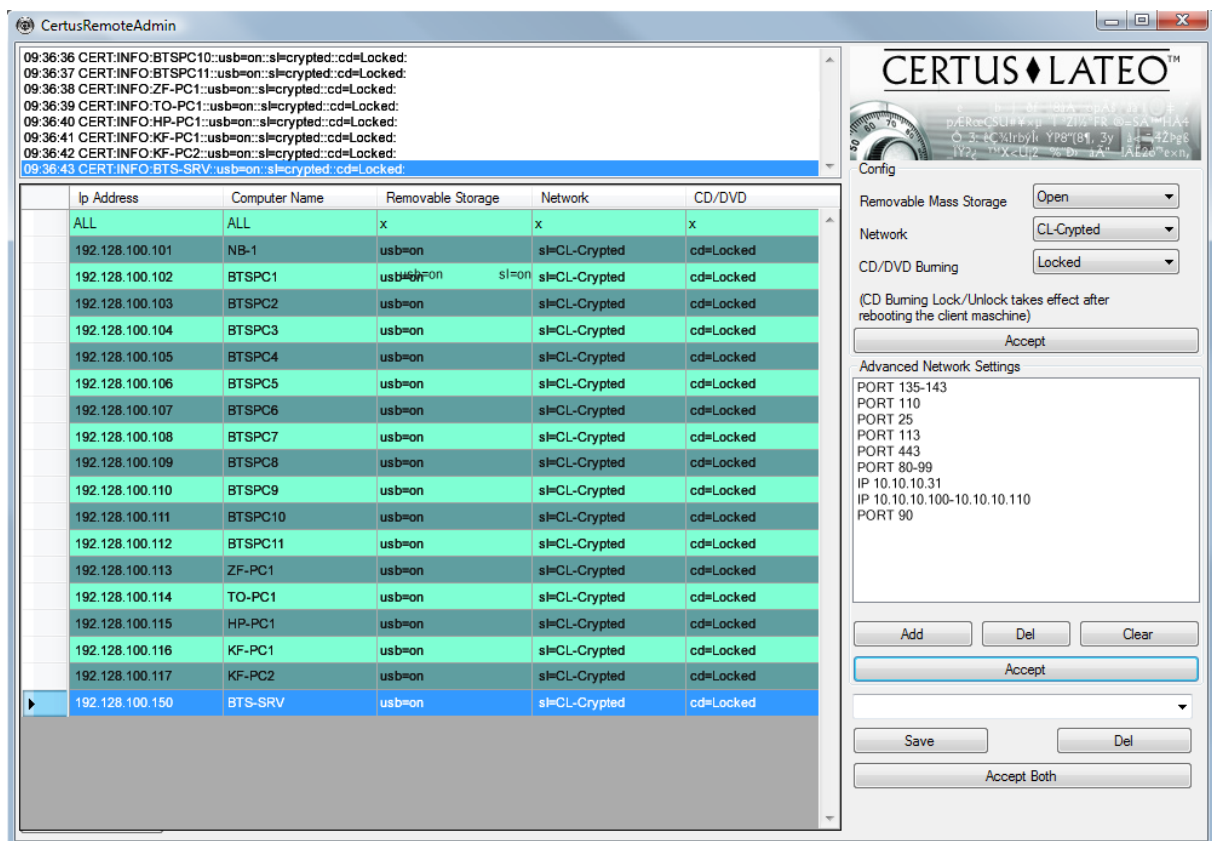
Nach der Eingabe des Administratorpasswortes muss der Dongle (USB Stick) innerhalb von maximal 60 Sekunden am entsprechenden Gerät eingesteckt werden. Andernfalls wird der Startvorgang wieder beendet.

Bei Systemen mit deaktiviertem USB Anschluss wird dieser für die Dauer der genannten Zeit vorübergehend freigeschaltet.

KONFIGURATIONEN

Nach dem Programmstart wird die Liste der dem Certus Lateo™ Umgebung angehörenden Systeme geladen.

Die Dauer bis zur Erstellung der vollständigen Liste ist abhängig von Grösse und Schnelligkeit des Netzwerkes.



PROTOKOLL

Das System Protokoll zeigt wichtige Ereignisse während der Arbeit mit dem Administrations Panel.

Durch drücken der rechten Maustaste wird ein Dialog geöffnet, über welchen das Protokoll in eine Text-Datei exportiert werden kann.

LISTE

Hier werden alle dem Certus Lateo™ Netzwerk angehörenden Geräte aufgelistet und die jeweiligen aktuellen Konfigurationen angezeigt.

Die Liste beinhaltet Angaben zu:

- IP Adresse
- Computer Name
- Aktuelle Konfiguration von USB Speicher, SD und MMC Karten, Netzwerkverbindung sowie CD/DVD Laufwerke.

CONFIG

Sobald ein Gerät in der Liste ausgewählt wurde werden im „Config“ Bereich die jeweiligen Einstellungen angezeigt. Diese können hier über die Auswahllisten geändert und mittels „Accept übernommen werden“.

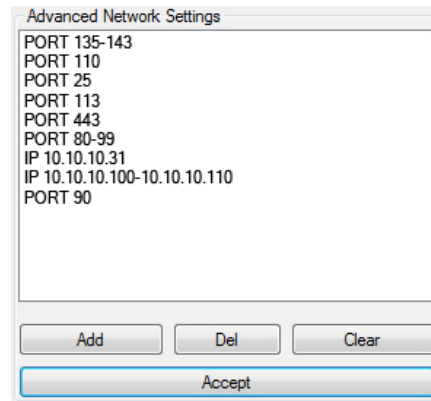
Bis zur Übernahme der Einstellungen auf den jeweiligen Geräten kann unter Umständen etwas Zeit vergehen.

Wichtig: USB Massenspeicher müssen vor der Änderung der Konfiguration entfernt werden, damit die neuen Einstellungen übernommen werden können.

IP UND PORT SETTINGS

Die IP und Port Settings erlauben das Definieren von einzelnen IP Adressen, IP Bereichen, einzelnen Ports und Port-Bereichen über welche das System **unverschlüsselt** kommunizieren darf.

Diese werden zeilenweise eingetragen, als einzelne Zahl (z.Bsp. „80“) oder mittels „von/bis“ Definitionen (z.Bsp. „811- 827“)



Die vorgenommenen Einstellungen können in der Auswahlliste benannt und durch die Schaltfläche „Save“ gespeichert werden. So stehen Sie zu einem späteren Zeitpunkt für nachfolgende Konfigurationen zur Verfügung.

Mittels „Accept“ werden die angezeigten Einstellungen für das gewählte Gerät übernommen.

Anmerkung:

Nach dem Auswählen eines Gerätes werden die aktuellen Port Konfigurationen nicht angezeigt.

5. ANHANG

SYSTEMVORAUSSETZUNGEN

Certus Lateo™ kann unter jedem 32- oder 64-Bit Windows Betriebssystem ausgeführt werden. Vorausgesetzt werden jedoch die aktuellsten Versionen. Im folgenden sind alle Plattformen aufgeführt, auf denen Certus Lateo™ getestet wurde:

- Windows XP SP3 (Home, Professional)
- Windows 2003 Serverfamilie
- Windows 2008 Serverfamilie
- Windows Vista
- Windows 7

WEITERE VORAUSSETZUNGEN

Die unzähligen unterschiedlichen Hardwarekonfigurationen können verständlicherweise nicht alle getestet werden. Systembedingt sollten jedoch keine diesbezüglichen Probleme auftreten, wenn die Hardware den gängigen Standards entspricht.

ANHANG A: ENDUSER LIZENZVEREINBARUNG

BTSELV

LIZENZRECHTE, ENDBENUTZER-LIZENZVERTRAG FÜR CERTUS LATEO™ - SOFTWARE APPLIKATIONEN GEMÄSS LIEFERUMFANG

WICHTIG - BITTE SORGFÄLTIG LESEN:

Dieser Barclay Technologies - Endbenutzer-Lizenzvertrag ("BTSELV") ist ein rechtsgültiger Vertrag zwischen Ihnen (entweder als natürlicher oder juristischer Person) und Barclay Technologies (Schweiz) AG. Dieses BTSELV bestimmt Ihre Verwendung der CERTUS LATEO™ - Software sowie der zu der Software gehörigen Komponenten, und verwandten Produkten. Die Software enthält möglicherweise dazugehörige Medien und gedrucktes Material und Dokumentation im "Online-" oder elektronischen Format. Indem Sie das SOFTWAREPRODUKT installieren, kopieren oder anderweitig verwenden, erklären Sie sich einverstanden, an alle Bestimmungen dieses BTSELV gebunden zu sein. Falls Sie den Bestimmungen dieses BTSELV nicht zustimmen, sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu installieren oder zu verwenden.

Das SOFTWAREPRODUKT wird sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum. Das SOFTWAREPRODUKT wird lizenziert, nicht verkauft.

1. LIZENZBEFREIBUNG

Das SOFTWAREPRODUKT wird wie folgt lizenziert:

- Verwenden und Kopieren von "CERTUS LATEO™": Barclay Technologies räumt Ihnen das Recht ein, Kopien des SOFTWAREPRODUKTS CERTUS LATEO™ auf genau der in der gelösten Lizenz definierten Anzahl Computern, weltweit, auf dem gültigen lizenzierten Kopien desjenigen Betriebssystems ausgeführt werden, für welches das SOFTWAREPRODUKT entwickelt wurde (z.B. Windows XP®, Vista, Windows 7 etc.), zu installieren und zu verwenden.

- Sicherungskopien: Sie sind ausserdem berechtigt, die für Sicherungs- und Archivierungszwecke notwendigen Kopien genannter SOFTWAREPRODUKTE anzufertigen.

2. BESCHREIBUNG WEITERER RECHTE UND EINSCHRÄNKUNGEN

Vorabversions-Software

Falls eine Komponente des SOFTWAREPRODUKTS als "Vorabversion" oder "Betaversion" gekennzeichnet ist, stellt diese Komponente des SOFTWAREPRODUKTS Vorabversionscode dar und wird möglicherweise vor Erscheinen der Lieferungs-/Veröffentlichungsausgabe grundlegend geändert. Sie sind nicht berechtigt, eine solche Komponente in einer realen Betriebsumgebung zu verwenden, in der sie genauso zuverlässig funktionieren muss wie ein Lieferungs-Endprodukt oder wo mit Daten gearbeitet wird, die nicht ausreichend gesichert wurden.

Urheberrechtshinweise

Sie sind verpflichtet, Urheberrechtshinweise auf allen Kopien des SOFTWAREPRODUKTS anzubringen und dürfen diese nicht ändern.

Vertrieb

Sie sind nicht berechtigt, Kopien des SOFTWAREPRODUKTS an Dritte weiterzugeben, ausser in der in Abschnitt 1 ausdrücklich gestatteten Form oder ausdrücklicher schriftlicher Erlaubnis.

Verbot im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung

Sie sind nicht berechtigt, das SOFTWAREPRODUKT zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Beschränkung, dies ausdrücklich gestattet.

Bemühungen zum Knacken der beim SOFTWAREPRODUKT verwendeten Verschlüsselungen oder der durch das SOFTWAREPRODUKT verschlüsselten Daten sind nicht gestattet.

Vermietung

Sie sind nicht berechtigt, das SOFTWAREPRODUKT zu vermieten, zu verleasen, zu verleihen oder zu verkaufen.

Übertragung

Sie sind berechtigt, alle Ihre Rechte aus diesem BTSELV auf Dauer zu übertragen, vorausgesetzt, der Empfänger stimmt den Bedingungen dieses BTSELV in schriftlicher Form zu.

Supportleistungen

Barclay Technologies oder deren Vertriebsgesellschaften bietet Ihnen möglicherweise Supportleistungen in Verbindung mit dem SOFTWAREPRODUKT ("Supportleistungen"). Die Supportleistungen können entsprechend den BT-Bestimmungen und -Programmen, die im Benutzerhandbuch, der Dokumentation im "Online"-Format und/oder anderen von Barclay Technologies zur Verfügung gestellten Materialien beschrieben sind, genutzt werden. Jeder ergänzende Softwarecode, der Ihnen als Teil der Supportleistungen zur Verfügung gestellt

Sicherheitsvorkehrungen

Bitte beachten Sie, dass sämtliche Daten während der Übermittlung mittels eines sicheren Krypt-Algorithmus verschlüsselt und somit in eine für Angreifer unlesbare Form gebracht werden. Ausschliesslich dem Sender sowie dem direkt angesprochenen Empfänger sind die notwendigen Entschlüsselungsmethoden bekannt, um die Daten wieder in den Originalzustand zu bringen.

Verschlüsselte Daten können Lizenz und/oder Crypto-Satz bezogen sein und ausschliesslich mit den bei der Verschlüsselung verwendeten Versionen wieder lesbar sein.

wird, wird als Bestandteil des SOFTWAREPRODUKTS betrachtet und unterliegt den Bestimmungen und Bedingungen dieses BTSELV. Barclay Technologies ist berechtigt, die technischen Daten, die Sie Barclay Technologies als Teil der Supportleistungen zur Verfügung stellen, für geschäftliche Zwecke, einschliesslich der Produktunterstützung und -entwicklung, zu verwenden. Barclay Technologies verpflichtet sich, solche technischen Daten ausschliesslich anonym im Sinne des Datenschutzes zu verwenden.

3. BEACHTUNG ALLER ANWENDBAREN GESETZE

Sie sind verpflichtet, das SOFTWAREPRODUKT nur in Übereinstimmung mit allen anwendbaren schweizerischen, den jeweiligen Nationalen und internationalen Gesetzen zu verwenden. Insbesondere der für Sie geltenden nationalen Bestimmungen im Bezug auf Verschlüsselungstechnologien.

4. KÜNDIGUNG

Unbeschadet sonstiger Rechte ist Barclay Technologies berechtigt, dieses BTSELV zu kündigen, sofern Sie gegen die Bestimmungen und Bedingungen dieses BTSELV verstossen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien des SOFTWAREPRODUKTS zu vernichten.

5. EIGENTUM

Jegliche Eigentumsrechte, einschliesslich, jedoch nicht beschränkt auf das Urheberrecht, an dem und in Bezug auf das SOFTWAREPRODUKT und jeder Kopie davon liegen bei Barclay Technologies, deren Vertriebspartner oder Lieferanten. Eigentumsrechte und geistiges Eigentum am und in Bezug auf den Inhalt, auf den durch das SOFTWAREPRODUKT zugegriffen wird, liegen beim jeweiligen Eigentümer und können durch entsprechende urheberrechtliche oder andere Gesetze über geistiges Eigentum geschützt sein. Dieses BTSELV gibt Ihnen keine Rechte an solchem Inhalt. Alle nicht ausdrücklich eingeräumten Rechte bleiben Barclay Technologies vorbehalten.

6. AUSFUHRBESCHRÄNKUNGEN

Hiermit stimmen Sie zu, dass Sie dieses SOFTWAREPRODUKT nicht in ein Land, an eine Person, eine juristische Person oder an Endbenutzer/innen, der/die/das den durch die Schweiz verhängten Ausfuhrbeschränkungen unterliegt, exportieren oder reexportieren werden. Sie geben hiermit die Gewähr und erklären, dass weder das schweizerische Amt für Exportgenehmigungen noch eine andere Bundesbehörde Ihre Exportgenehmigung ausgesetzt, widerrufen oder abgelehnt hat.

7. GEWÄHRLEISTUNGS AUSSCHLUSS

Barclay Technologies schliesst ausdrücklich jede Gewährleistung für das SOFTWAREPRODUKT aus. Das SOFTWAREPRODUKT und die darauf bezogene Dokumentation wird Ihnen "so wie sie ist" zur Verfügung gestellt, ohne Gewährleistung irgendeiner Art, weder ausdrücklich noch konkludent, einschliesslich, aber nicht beschränkt auf konkludente Gewährleistungen der Tauglichkeit, der Eignung für einen bestimmten Zweck oder des Nichtbestehens einer Rechtsverletzung. Das gesamte Risiko, das sich aus dem Verwenden oder der Leistung des SOFTWAREPRODUKTS ergibt, verbleibt bei Ihnen.

8. BESCHRÄNKTE HAFTUNG

Bis zum durch anwendbares Recht äusserstenfalls Zulässigen, können weder Barclay Technologies noch deren Vertriebsgesellschaften, Vertriebspartner oder Lieferanten haftbar gemacht werden für irgendwelche besonderen, zufällig entstandenen oder indirekten Schäden oder Folgeschäden (einschliesslich, aber nicht beschränkt auf entgangenen Gewinn, Betriebsunterbrechung, Verlust geschäftlicher Informationen oder irgendeinen anderen Vermögensschaden), die aus dem Verwenden oder der Unmöglichkeit, das SOFTWAREPRODUKT zu verwenden, oder durch die Leistung bzw. Nichtleistung von Supportleistungen entstehen, und zwar auch dann, wenn Barclay Technologies zuvor auf die Möglichkeit solcher Schäden hingewiesen worden ist. In jedem Fall bleibt Barclay Technologies gesamte Haftung auf den Betrag von sFr. 100, oder auf sFr. 0.00,- beschränkt, wobei der kleinere Betrag massgebend ist. Falls Sie jedoch mit Barclay Technologies einen Vertrag über Supportleistungen abgeschlossen haben, wird Barclay Technologies gesamte Haftung in Bezug auf Supportleistungen durch die Bestimmungen dieses Vertrags festgelegt.

9. VERSCHIEDENES

Da einige Staaten/Gerichtsbarkeiten den Ausschluss oder die Begrenzung der Haftung für Folge- oder zufällig entstandene Schäden nicht gestatten, gilt die vorstehende Einschränkung möglicherweise nur in dem jeweiligen Gesetz entsprechenden Rahmen.

Sollten eine oder mehrere Bestimmungen dieses Vertrages aus irgendwelchen Gründen unwirksam sein oder werden, wird davon die Gültigkeit des Vertrages im Ganzen nicht berührt. Vielmehr verpflichten sich die Vertragspartner, anstelle der unwirksamen Bestimmungen eine ihrem wirtschaftlichen Zweck entsprechende wirksame Regelung zu vereinbaren. Und zwar so, dass der gemäss den rechtsunwirksamen Teilen angestrebten Zweck so weit als möglich erreicht/erfüllt wird.

Dieses BTSELV untersteht dem schweizerischen sowie dem internationalen materiellen Recht.

Erfüllungsort und Gerichtsstand ist Zürich (Schweiz)

Indem Sie das SOFTWAREPRODUKT installieren, kopieren oder anderweitig verwenden, erklären Sie sich einverstanden, die im Inhalt der Übergabedokumentation beschriebenen Softwareprodukte/-Dienstleistungen im Lieferumfang vollständig und abschliessend gemäss Auftragserteilung erhalten zu haben.

Urdorf, 1. Oktober 2009

Warnung

Das beschriebene Computerprogramm ist weltweit urheberrechtlich geschützt. Sie sind nicht berechtigt, das Programm bzw. Teile davon ohne ausdrückliche Genehmigung des Herstellers zu reproduzieren oder weiterzugeben. Widersächliche Handlungen können eine zivil- oder strafrechtliche Ahndung nach sich ziehen und werden gemäss der geltenden Rechtsprechung mit grösstmöglicher Härte verfolgt.

Das vorliegende Benutzerhandbuch ist urheberrechtlich geschützt. Es darf weder kopiert, noch in irgendeiner anderen Weise reproduziert werden. Es darf in keiner Form, auch nicht auszugsweise verbreitet oder in eine andere Sprache übersetzt werden.

Der Inhalt dieser Dokumentation ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Herausgeber kann keine Verantwortung oder sonstige Haftung für Folgen übernehmen, die auf unvollständige oder fehlerhafte Angaben in diesem Benutzerhandbuch zurückzuführen sind.

Alle Rechte Vorbehalten.